جامعة محمد خيضر - بسكرة
كلية الحقوق والعلوم السياسية
مخبر أثر الاجتهاد القضائي على حركة التشريع

سلسلة مطبوعات المخبر



الجريمة المعلوماتية

دراسة تأصيلية مقارنة

الدكتور: يعيش تمام شوقي
أستاذ محاضر . أ .

الدكتور: يعيش تمام شوقي

الجريمة المعلوماتية

طبعة 2019


mohamed khatab



سلسلة مطبوعات المخبر

جامعة محمد خيضر - بسكرة
كلية الحقوق والعلوم السياسية
مخبر أثر الاجتهاد القضائي على حركة التشريع

الجريمة المعلوماتية

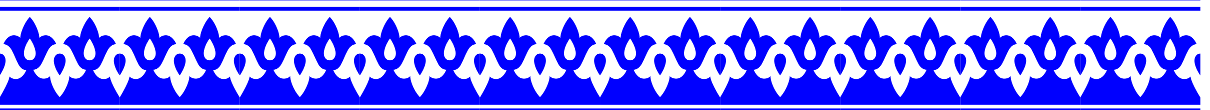
(دراسة تأصيلية مقارنة)

الدكتور يعيش تمام شوقي

أستاذ محاضر "أ" كلية الحقوق والعلوم السياسية

جامعة بسكرة- الجزائر

جانفي 2019



سلسلة مطبوعات المخبر (06)

العنوان: الجريمة المعلومــاتية

(دراســة تأصيلية مقارنة)

المؤلف: د. شوقي يعيـش تمام

عدد الصفحات: 134 صفحــــــة

ردمك: ISBN 978-9931-9454-4-4

الإيــداع القــانوني: السداســي الأول 2019

الطبعة الأولـى – جانفي 2019

مطبعة الرمال (الوادي) – الجزائر



مخبر أثر الاجتهاد القضائي على حركة التشريع ـــــــــ جامعة محمد خيضر بسكرة



قال الله جل جلاله

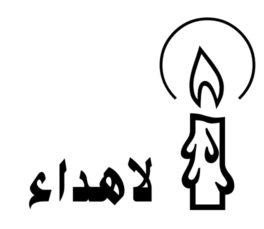
بسم الله الرحمن الرحيم

ولكل درجات مما عملوا وما ربك

بغافل عما يعملون

الآية 132 من سورة الأنعام





لاهداء

أهدي ثمرة هذا العمل إلى:

والدي رحمه الله... طيب اللــــه ثراه

أمي الغـــــالية ... حفظها وأطال الله عمرها

زوجتي وأبنائي الأفاضل ... أدامهـــــم الله ذخرا لي

أخـــــــــوتي ... رعـــــــاهم اللـــــــه

رفقاء دربي وزملائي بكلية الحقوق بجامعة بسكرة وفقهم الله دومــــا

إلى كل باحث علم نزيه

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، نحمده حمدا كثيرا غير منقطع على منِّه وتوفيقه وإحسانه لإتمام هذا المؤلف.

لا بد لي في المقام الأول أن أن أتقدم بجزيل الشكر والعرفان وعظيم التقدير والامتنان إلى الأستاذ الدكتور بن مشري عبد الحليم تقديرا لما بذله ومنحنا من فكره الواسع وجهده الكبير في تنقيح وتنظيم هذا المؤلف والحرص على إخراجه في أحسن صورة ، فكان له بذلك كبير الإسهام في إنجازه.

كما أتقدم بالشكر الوافر إلى الزميل والأخ المحترم الدكتور محمد خيلفة على دعمه المتواصل لي لانجاز هذا المؤلف، والذي لم يدخر هو الآخر أي جهد في تزويدي بالمراجع التي استفدت منها بالقسط الوافر ، فجعل الله كل ذلك في ميزان حسناته.

الدكتور شوقي يعيش تمام

أستاذ محاضر "أ" - جامعة بسكرة



مقدمة

لا مراء في أن الواقع المعاش يعرف تسارعا غير مسبوق في أنظمة ومسار التطور العلمي والتكنولوجي ما أدى الى ثورة تكنولوجية ومعلوماتية كان من إفرازاتها التوسع الكبير والمستمر في استخدام وسائل وتقنيات الاتصال والاعلام في مختلف مجالات الحياة الخاصة والعامة في ظل ما أصبح يختزل في مسمى البيئة الرقمية أو بيئة المعلوماتية.

وبقدر ما أصبحت تمثله هذه البيئة الجديدة من ضرورة وحتمية للنشاط الانساني الفردي وشبكة العلاقات الاجتماعية الخاصة بين الأفراد أو بينهم وبين مؤسسات الدولة تحت طائلة الحكومة الالكترونية وما يمكن أن تسفر عنه هذه الأخيرة من تقديم وتوصيل الخدمات ذات الطابع الشخصي أو المعرفي أو الاداري في أسرع وقت وأقل تكلفة، وأيسر الطرق، وبدقة عالية، إلا أن ذلك رافقه في الوقت ذاته الانحراف في التعامل مع معطيات الأنظمة المعلوماتية على مختلف أنواعها، فأضحت مجالاً مفتوحا لتنامي التهديدات والانتهاكات الناتجة عن استغلال الوسائط المعلوماتية في مجالات الحياة المختلفة على نحو ما يضر بالمصالح الخاصة للأفراد، كانتهاك سرية الحياة الخاصة أو سرية الحسابات الالكترونية، أو حتى المصالح العامة لمؤسسات الدولة كتزوير البيانات والمعطيات المعلوماتية أو أعمال التجسس والاتلاف والتحويل.

لذلك كان لزاما على المشرع في كل دولة، وفي الجزائر على وجه الخصوص أن يتدخل من تأجل تأطير الأفعال والوقائع التى ترتكب بشكل متصاعد ومتفاوت مستفيدة في ذلك مما أفرزته التطورات التكنولوجية من وسائط معلوماتية مفتوحة للجمهور، فترقى لتشكل أعمالا إجرامية بمفهوم قانون العقوبات، أو القوانين المكملة له، فظهر بذلك مصطلح الجريمة المعلوماتية

بوصفها جرائم حديثة تتميز في طبيعتها وكيفية إرتكابها عن سائر الجرائم التقليدية الأخرى.

يمكن القول في هذا السياق أن وجود نظام قانوني للجرائم المعلوماتية في كل دولة فرضته عدة متغيرات يأتي في صدراتها عدم القدرة على مجابهة ومواجهة المخاطر والأضرار الناتجة عن الحماية التقنية المحدودة المقررة لأنظمة المعلوماتية، ولكن الصعوبة لا تزال تطرح في كل مرة حتى مع وجود نظام تجريمي لردع الانتهاكات المرتبطة باستخدام أنظمة المعلومات والاتصال خاصة مع ازدياد وتنوع تقنيات توظيفها، وبذلك أصبحت العلاقة طردية بالضرورة بين تطور أنظمة المعلوماتية من جهة، والاجرام المعلوماتي من جهة أخرى. الأمر الذي أضحى معه موضوع الجرائم المعلوماتية من المواضيع الأكاديمية ذات الأهمية البالغة المرتبطة بعدة صعوبات وعوائق تحد من مكافحتها خاصة مع اختلاف نظرة المشرع الجنائي الداخلي في كل دولة حول نطاق العناصر المكونة لها.

ومن هنا اتجهت جهود الدول نحو البحث عن آليات مشتركة لتنسيق المواقف والالتفاف حول سبل للتعاون الدولي بما يسمح بالتقليل من مخاطر ومضار الاجرام المعلوماتي بعدما كشفت التجربة عدم كفاية القواعد المقررة على المستوى الداخلي لمكافحة هذا النوع من الجرائم.

ومهما يكن من أمر فإننا نتطلع من خلال هذا المؤلف الاحاطة بالاطار النظري والتأصيلي للجريمة المعلوماتية ورصد أهم الاشكالات القانونية والعملية التي تعترض سبيل مكافحتها.

وقد رأينا من المهم والمفيد أن يتم تناول هكذا موضوع من خلال قسمين رئيسين، يتطرق الأول الى الاطار المفاهيمي والتأصيلي للجريمة المعلوماتية، أما

الثاني فيركز على الاشكالات التي تعترض مواجهة الجريمة المعلوماتية في أبعادها المختلفة.

الفصل الأول

الإطار المفاهيمي والتأصيلي

للجريمة المعلوماتية

الفصل الأول

الاطار المفاهيمي والتأصيلي للجريمة المعلوماتية

هناك تلازم حتمي بين مستوى تطور نظام المعلوماتية وما يرتبط به من وسائل وتقنيات، وبين دقة الاطار القانوني المتعلق بمكافحة الاجرام المعلوماتي ذلك أن الوعي بمخاطر ومضار المعلوماتية على المصالح الاجتماعية المختلفة من شأنه أن يضع أمام المشرع تصورا واضحا بما يسمح له بتأطير الأفعال التي يمكن أن تحمل وصف الجريمة المعلوماتية، باعتبارها أفعال مستحدثة تتميز بالضرورة عن غيرها من الأفعال المكونة للجرائم الأخرى الواقعة على الأشخاص أو الأموال، وهو ما من شأنه أن يخفف من حدة تزايد خطر الاجرام المعلوماتي خاصة مع عدم إمكانية القضاء عليه بشكل نهائي.

وعلى هذا الأساس آثرنا أن نستهل الفصل الأول بتحديد الأحكام النظرية والتأصيلية المرتبطة بجرائم المعلومات على اعتبار أنها مادة أولية ضرورية لضبط الاطار القانوني الموضوعي الذي يحكمها، وهو ما يتأتى من خلال التعرض مدلول الجريمة المعلوماتية (المبحث الأول) والاشكالات المقترنة بمكافحتها(المبحث الثاني).

المبحث الأول

ضبط مدلول الجريمة المعلوماتية وطرفيها

لم تحض موضوع الجريمة المعلوماتية بموقف مشترك بين غالبية الفقهاء والمختصين حول دلالة إطلاق وصفها وما يرتبط بها من معايير، وهو الأمر الذي يفسر تعدد التجاذبات الفقهية وعدم الاتفاق على معيار جامع مانع حول نطاقها الموضوعي (الأفعال المكونة لها) والشخصي (مرتكب الجريمة)، وهذا مقارنة ببعض الجرائم الأخرى المؤطرة بموجب قانون العقوبات أو القوانين المكملة له. وحتى يتسنى لنا ضبط مدلول الجريمة المعلوماتية وفقا لهذا الطرح يكون من المهم التطرق إلى ضبط مدلولها وطرفيها وهما المجرم والضحية في مبحث أول، أما المبحث الثاني فنخصصه لتحديد خصائص وسمات الجريمة المعلوماتية.

المطلب الأول: تعريف الجريمة المعلوماتية

قبل التطرق إلى تحديد أهم التعاريف التي أدلى بها الفقه بخصوص الجريمة المعلوماتية من الضروري والمفيد استحضار أهم المفاهيم والمصطلحات المرتبطة بحقل المعلوماتية والتي كثيرا ما تستخدم بمناسبة الحديث عن الاجرام المعلوماتي، وذلك على النحو التالي:

أولا - تقنية المعلومات:

يقصد بها عملية تغذية ومعالجة وتخزين، ثم بث واستخدام المعلومات الرقمية والنصية والمصورة والصوتية عن طريق تقنيات الحاسب الآلي والاتصالات، وبالتالي فهي تتضمن توظيف أدوات وأساليب، وتجهيزات متطورة لنقل المعلومات من المرسل الى المستقبل بأقل وقت وجهد وتكلفة، وبأقصى قدر من

الدقة[1].

ثانيا- البيئة الرقمية:

يعبر مفهوم البيئة الرقمية عن مرحلة من التحول من البيئة التقليدية إلى بيئة جديدة تحل فيها مستودعات المعلومات الالكترونية محل المطبوعات والأرصدة الورقية، ويتغير من خلالها طبيعة الاجراءات والعمليات التي يتم فيها التعامل مع هذه الأرصدة ووسائل حفظها ونقلها، بالإضافة إلى تبدل في ملامح الخدمات التي يتم تقديمها من خلال تطور طرق اتاحة المعلومات وتمكين طالبيها من الحصول عليها وبهذا يمكن القول أن البيئة الرقمية مفهوم أفرزته التطبيقات التكنولوجية المختلفة في تفاعل الانسان، ومدى تقبله للتغيرات التكنولوجية الجديدة[2].

ثالثا - الأمن المعلوماتي:

يقصد بأمن المعلومات من الزاوية الأكاديمية ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن الاعتداء عليها، ومن الزاوية التقنية هو مجموعة الوسائل والأدوات والاجـــراءات اللازم توفيرها لضمـــان حمـــاية المعلـومات من مختلف الأخطار

---

[1] – منصور بن سعيد القحطاني، مهددات الأمن الالكتروني وسبل مواجهتها، رسالة ماجستير في العلوم الادارية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2008، ص 17.

[2] – لحواطي عتيقة، استرجاع المعلومات العلمية والتقنية في ظل البيئة الرقمية ودوره في دعم الاتصال العلمي بين الباحثين، رسالة دكتوراه LMD في علم المكتبات، معهد علم المكتبات والتوثيق، جامعة قسنطينة، 2014/2013، ص 49.

الداخلية والخارجية[1].

وبالجمع بين المفهومين الأول والثاني يمكن القول أن أمن المعلومات ينصرف مدلوله إلى جملة الاجراءات الادارية والفنية المتخذة لحماية الأجزاء المادية لمكونات الحاسب الآلي من أجهزة وملحقات وشبكات ووسائل اتصال، وأقراص صلبة ومرنة وضوئية، وكذا حماية الأجزاء غير المادية كالبرامج والتطبيقات والبيانات والمعلومات من السرقة والتلف المتعمد، أو التخريب أو التبديل، أو الاختراق وغيرها...[2].

مما تقدم يتبين لنا أن الأمن المعلوماتي قد أضحى فكرة ضرورية في إطار تفعيل السياسة الجنائية الوقائية لمنع ارتكاب مزيد من جرائم المعلوماتية بعدما كشفت التجربة أن السياسة الجنائية الردعية وحدها عاجزة عن مكافحتها ووضع حد لانتشارها، وقد عرف هذا الأمر رواجا أكثر في مجال حماية التجارة الالكترونية من مختلف المخاطر التي تهددها، وكان الهدف من ذلك هو حماية المواقع الخاصة على الانترنت من خلال أنظمة المتاجر الافتراضية، وكذلك حماية المعاملات المالية الالكترونية من خلال نظام الوفاء الالكتروني، إلى جانب نظام حافظة النقود الالكترونية الافتراضية ونظام التشفير[3]، وقـد تعدى الأمر

---

[1]- ليتيم فتيحة، ليتيم نادية، "الأمن المعلوماتي للحكومة الالكترونية وارهاب القرصنة"، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 12، ص 239.

[2]- منصور بن سعيد القحطاني، مرجع سابق، ص 20.

[3]- لمزيد من التفصيل حول هذا الموضوع أنظر: ضياء نعمان، "الحماية التقنية للتجارة الالكترونية"، مجلة قانون وأعمال، المطبعة والوراقة الوطنية، مراكش، المغرب، العدد 1، مارس 2011، ص 19 وما بعدها.

إلى حماية خصوصية المعلوماتية[1].

رابعا - شبكة الانترنت:

تعددت التسميات التي أطلقت على شبكة الانترنت من شبكة الشبكات إلى شبكة ما بعد الشبكات الى بيت العنكبوت الالكترونية، وعلى غرار تعدد التسميات، تعددت التعاريف الخاصة بها نذكر منها على سبيل المثال: الانترنت هي شبكة الشبكات التي تربط الأشخاص وأجهزة الكمبيوتر في جميع أنحاء الكرة الأرضية، فهي اتحاد شبكات الاعلام الآلي دون نواة مركزية يتم الوصول إليها بحاسوب يربط بحاسوب مركزي لمورد الأنترنت.[2]،

وتاريخيا ارتبط ظهور الانترنت بأواخر الستينات في الولايات المتحدة الأمريكية عندما شكلت وزارة الدفاع لجنة من الخبراء أوكلت أليهم مهمة انشاء شبكة تربط بين الحاسبات، ونجحت في مهمتها، وبذلك أنشئت أول شبكة للإنترنت تحت مسمى شبكة وكالة مشروع الأبحاث المتقدمة[3]

خامسا - النظام المعلوماتي:

نشير بداية أنه ليس هناك اتفاق عام حول توحيد هذا المصطلح، حيث أن هناك الكثير من المصطلحات التي يتم استخدامها، ويراد بها نفس المعنى وهو النظام المعلوماتي على غرار مصطلح المعالجة الآلية للمعطيات، ومنظومة معالجة كمبيوتر، ومصطلح معالجة آلية استعمل أول مرة في فرنسا لتنظيم حماية

---

[1] - راجع في هذا الصدد: محمد سيد سلطان، قضايا قانونية في أمن المعلومات والبيئة الالكترونية، دار ناشري للنشر الالكتروني، 2012، ص 24.

[2] - فندوشي ربيعة، الاعلان الالكتروني، دار هومة للطباعة والنشر والتوزيع: الجزائر، 2011، ص ص 87، 88.

[3] - لمزيد من التفاصيل حول الموضوع أنظر: محمد سيد سلطان، مرجع سابق، ص 7.

المعلومات الاسمية عن طريق القانون 6 يناير 1976، وكان وزير المالية الفرنسي قد قدم في المعجم الأبجدي تعريفا لفكرة النظام المعلوماتي بأنه مجموعة تجهيزات وبرامج يحتوي على الأقل على الأقل على حاسب آلي يقوم بمعالجة وارجاع البيانات، ران كان ما يؤخذ على هذا التعريف كونه قاصر ويهمل الروابط بين مختلف وسائل هذا المجموع الذي يشكل النظام[1].

أما اتفاقية بودابست لسنة 2001 فقد استخدمت اصطلاح منظومة كمبيوتر، واعتبرت بموجبه أنه أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات؛واعتبرت في ذات الوقت أن بيانات الكومبيوتر تتعلق بعمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر،بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة[2].

ومهما يكن من أمر فإن الفقه لم يشذ عن العناصر التي يتألف منها النظام المعلوماتي وفقا لما سبق بيانه فعرف تبعا لذلك على أنه مجموعة المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما، وفي سبيل ذلك يقبل مدخلات وينتج

---

[1] - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الطبعة الأولى، دار الجامعة الجديدة: الاسكندرية، ص ص 16، 17.

[2] - أنظر: المادة الأولى من الملحق المتعلق بالنص الكامل لاتفاقية بودابست لسنة 2001 المتعلقة بالجريمة الالكترونية.

مخرجات ويسمح باستقبال مدخلات مرتدة،[1]

بخصوص مفهوم الجريمة المعلوماتية لم يتفق جمهور الباحثين والدارسين وحتى التشريعات ت على مفهوم موحد يتضمن العناصر الأساسية المكونة للجريمة المعلوماتية، وهذا ما يفسره تعدد التسميات التي أطلقت عليها، فمنهم من يطلق عليها تسمية الجريمة الالكترونية، والبعض تسمية جرائم الانترنت، وجرائم الكمبيوتر، وذهب آخرون في تسميتها بجرائم المعالجة الآلية للبيانات والمعطيات[2].

ومهما يكن من أمر، فإن اختلاف وتعدد كل هذه التسميات لا يجب أن يغير من محتوى الجريمة المعلوماتية، لذلك آثرنا التركيز على بعض التعاريف، مع تبيان ما يؤخذ عليها بشكل مشترك، تمهيدا للخروج بتعريف جامع مانع للعناصر التي تتألف منها الجريمة المعلوماتية.

---

[1] - شوقي يعيش تمام، محمد خليفة، "نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري"، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، بيروت، لبنان، العدد 25، ماي 2018، ص 17.

[2] - وقد استخدم المشرع الجزائري هذه التسمية بعنوان القسم السابع مكرر من قانون العقوبات المضاف بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، ويتضمن المواد من 394 مكرر الى 394 مكرر 7، وحدد من خلالها ثلاث أنواع من جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي:

- جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي.
- جريمة التلاعب بالمعطيات والبيانات المعلوماتية.
- جريمة التعامل غير المشروع في معطيات لارتكاب جريمة معلوماتية.

حيث ذهب البعض في تعريفها على أنها: "كل سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، وهي على رأي البعض الآخر " كل نشاط غير مشروع موجه لنسخ أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[1].

وإذا كانا التعريفين السابقين يركزان على موضوع الجريمة المعلوماتية، فهناك من فضل التركيز في تعريفها على وسيلة ارتكابها، وتبعا لذلك عرفت الجريمة المعلوماتية بأنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب"، وهي أيضا: "نشاط اجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة أو غير مباشرة بهدف تنفيذ العمل الاجرامي المقصود"، وفي نفس السياق يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسا في ارتكابها"[2]، ويقترب هذا التعريف الأخير من تعريف الفقيهين TATIY.R, HAND COTEL عندما اتفقا على أنها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب الآلي[3].

وزيادة على كون الحاسوب وفقا لما تقدم هو وسيلة الجريمة فقد يكون كذلك هو المسهل للجريمة، وعليه يعتبر جهاز الحاسوب كوسيلة عندما ننظر الى

---

[1]- عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة الكوفة، مركز دراسات الكوفة (العراق)، العدد السابع، 2008، ص 113.

[2]- مشتاق طالب وهيب، "مفهوم الجريمة المعلوماتية ودور الحاسب بارتكابها"، مجلة العلوم القانونية والسياسية، جامعة ديالي، (العراق)، المجلد الثاني، العدد 1، 2014، ص 338.

[3]- سميرة معاشي، "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، قسم الكفاءة المهنية للمحاماة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد السابع، 2010، ص 276.

العلاقة بين الجاني والضحية (Criminel / Victime)، وكمسهل للجريمة عندما ننظر الى العلاقة بين الجاني والجاني (Criminel / Criminel)، والفرق بين هاتين الفئتين هي مسألة درجات، ويمكن للحاسوب أن يؤدي وظيفة مزدوجة في جريمة واحدة، مثال ذلك الغش في التجارة الالكترونية عبر الانترنت (وسيلة)، أو تبادل الاتصالات بين المجرمين(مسهل)[1].

إن أهم ملاحظة يمكن استخلاصها من استقراء كل التعاريف السابقة بخصوص الجريمة المعلوماتية أنها تتقاطع في اعتبار أن مناط ارتكابها يتم بواسطة الكمبيوتر أو الحاسوب في الوقت الذي يتبين لنا أن جهاز الكمبيوتر ليس الوسيلة الوحيدة المستخدمة في ظل ما يشهده العالم من ثورة اتصالات معلوماتية هائلة أفرزت أنماط ووسائل اتصال جديدة لتبادل نظم المعلوماتية على غرار الهواتف المحمولة، وآلات السحب الآلي للأموال، وما يرتبط بها من بطاقات الكترونية معدة لهذا الغرض وغيرها...

فضلا على أن الجريمة المعلوماتية ومثلما أنها تنال من معطيات وبيانات وبرامج الحاسب الآلي من خلال عمليات التحويل والنقل والحذف والتعديل، فإنها تتضمن كذلك عمليات الاعتداء المادي كإتلاف مكونات ومشتملات الأجهزة المستعملة في إطار المعالجة الآلية للمعطيات والبيانات، وبناءا على ذلك نقترح في تعريف الجريمة المعلوماتية: "هي كل سلوك يتضمن تهديدا واضحا أو ضررا يمس بمصالح خاصة للأفراد أو عامة للدولة بمناسبة استخدام نظم المعلوماتية في إطار المعالجة الآلية للمعطيات والبيانات، والتي ينتج عنها حتما عمليات

---

[1] - راجع بخصوص هذا الموقف: غنية باطلي، الجريمة الالكترونية -دراسة مقارنة-، الدار الجزائرية للنشر والتوزيع: الجزائر، 2015، ص 15.

الاتلاف المادي لمكونات تلك الوسائل أو تعطيل استخدامها، مثلما قد ينتج عنها تغيير وتعديل محتوى البرامج والمعطيات والبيانات، أو حذفها واتلافها".

يتضح مما تقدم أن الاعتداء الذي يقع في نطاق الجريمة المعلوماتية يتعلق أساسا بمكونات الحاسب الآلي المادية منها، غير المادية، وما يمكن أن يقوم مقامه. ويذهب البعض إلى اعتبار أن الجرائم المعلوماتية قد تقع على الحاسب الآلي ذاته، وما يتصل به من ملحقات، وقد تقع على مال الغير باستخدام الحاسب ذاته، ومن أمثلة هذه الحالة الأخيرة التجسس والتنصت على الأفراد والاعتداء على حياتهم الخاصة سواء بالتصوير أو التسجيل، السرقة من الأرصدة في البنوك ونحو ذلك، ولا شك أن الفاعل في هذا الحالات هو مستخدم الحاسب الآلي، أما الجهاز فليس إلا وسيلة لارتكاب الجريمة التي يتمثل محلها في الحق الذي تم المساس به[1].

أما الحالات التي يكون فيها النظام الآلي موضوعا للجريمة فتتمثل في الاعتداءات التي تقع على النظام الآلي ذاته وما يتصل به من أدوات وأجهزة، فمثل هذه الأموال أن تعرضت لاعتداء من أجل اتلافها فإن النصوص الجزائية القائمة في القانون الجنائي، كنصوص الاتلاف كفيلة بحمايتها لأن الأمر يتعلق بمال مادي وفقا للمفهوم الذي درج عليه الفقه للمال، أما بالنسبة للجانب غير المادي للنظام الآلي فقد يتعرض لصور خاصة من الاعتداءات كنسخ البرامج أو تقليدها أو تدميرها، أو تعطيلها أو تزوير المستخرجات الالكترونية أو إفشاء

[1] - محمد حماد مرهج الهيتي، الجريمة المعلوماتية -دراسة مقارنة في التشريع الاماراتي والسعودي والبحريني والقطري والعماني-، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2014، ص 73.

محتوياتها،فمثل هذه الاعتداءات تأتي النصوص الجزائية العامة قاصرة عن علاجها بسبب الطبيعة الخاصة لهذا الجانب أو الكيان[1].

المطلب الثاني: المجرم والضحية (طرفي الجريمة المعلوماتية)

يرتبط ارتكاب جرائم المعلومات في أي زمان ومكان بما يعرف بالمجرم المعلوماتي[2]، وهناك من يتوسع في تحديد فئات المجرم المعلوماتي تبعا للخطورة الاجرامية الكامنة فيه، إلا أننا نرى من جانبنا وعلى غرار ما يتمسك به كثير من الباحثين بأن التركيز يجب أن ينصب على فئتين هما:

الفئة الأولى (Haker):

وهم فئة المجرمين الأقل خطورة والذين تتوافر لديهم خبرة معتبرة في مجال الحاسب الآلي ووظائفه ومكوناته، ونظم المعلوماتية، ومعرفة البرامج التي يجري العمل بها كالبرامج المحاسبية، وبما أن هؤلاء يمارسون مواهبهم لغرض الولوج الى نظم المعلومات بدافع الفضول أو اللهو، فهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي اليها أفعالهم غير المشروعة، لذلك فأن هذه

---

[1]- محمد حماد مرهج الهيتي، مرجع سابق، ص 74.

[2]- يرجع الفضل في الكشف عن مصطلح المجرم المعلوماتي إلى كاتب الخيال العلمي الأمريكي "وليم جيبسون" في مؤلفه الصادر سنة 1984، وعليه فإن مصطلح المجرم المعلوماتي فكرة جديدة على الفقه الجنائي، ففي جرائم المعلومات لسنا بصدد سارق أو محتال عادي ولكننا بصدد مجرم ذو مهارة تقنية عالية ودراية بالنظام المستخدم في الحاسوب، وهذه المهارة هي التي تمكنه من اختراق الحسابات البريدية، والأنظمة الالكترونية المحمية، أو اتلاف البيانات أو محوها.../ أنظر في هذا الصدد: رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011، 2012، ص 55.

الفئة تعد أقل خطورة، ولكن مع ذلك يلاحظ أن ازدياد الأعداد المستخدمة لتكنولوجيا الاعلام والاتصال، وما يتبعه من ازدياد نسبة الجرائم في هذا المجال، فلا يستبعد معه احتمال انزلاق هذه الفئة من مجرد هواة للأفعال غير المشروعة إلى محترفين[1].

الفئة الثانية (Crackers):

أصحاب هذه الفئة يتمتعون بمستوى مهاري عالي يسمح لهم بالدخول واقتحام الأنظمة الحاسوبية بكل سهولة واقتدار رغم احتياطات الأمن المتعددة، ورغم قلة العناصر القادرة على اكتشافها، مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، إذ غالبا ما تكون جرائم التحويل والنسخ والاضافة للمعلومات على البرامج وتغيير محتواها من جانب هذه الفئة ضخمة[2]

وتبعا لذلك يميز بين مصطلحي Crasher وLe cracker من حيث نتيجة الفعل الاجرامي، فالأول يلج داخل النظام ويحطم المعطيات بدافع الرغبة، أما الثاني فيدخل الى النظام للتحريف في هذه المعطيات أو محوها أو ادخال معلومات أخرى، كما يطلق على فئة Cracker بـ: Spiders لأنهم يعملون في الخفاء، ولا يتركون آثارا مادية لأفعالهم، وقد يصبحوا أشد خطورة إذا ما تم تبادل تقنياتهم فيما بينهم، وشكلوا ما يعرف بالجماعات أو الفرق المتخصصة أو العمل عن طرق الوساطة[3].

---

[1] - أنظر على التوالي: محمد علي سالم، حسون عبيد هجيج، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الانسانية جامعة بابل(العراق)، المجلد 14، العدد 3، 2008، ص 89./ رصاع فتيحة، مرجع سابق، ص ص 56، 57، 58.

[2] - راجع في هذا الصدد: محمد علي سالم، حسون عبيد هجيج، مرجع سابق ص 89.

[3] - غنية باطلي، مرجع سابق، ص ص 38، 39.

والتاريخ حافل بالأسماء الذين تم القبض عليهم بعد عدة محاولات، ومن أشهرهم في الولايات المتحدة الأمريكية كيفين ميتنينك الذي قام بسرقات كثيرة من أشهرها سرقة الأرقام الخاصة ب 20000 بطاقة إئتمان، وقد تم القبض عليه والحكم عليه بالسجن لمدة عام، ولكنه لم يخرج من السجن على اعتبار أنه مجرم خطير ولا توجد شبكة لا يستطيع إختراقها، وقد تعالت الأصوات المطالبة بالإفراج عن كيفين، كما ظهرت جماعات تقوم بعمليات قرصنة باسمه[1].

أما بخصوص المجني عليه (الضحية) في جرائم المعلومات، فمن المتصور أن يقع ضحية جرائم المعلومات جميع الأشخاص سواء الطبيعية أو المعنوية العامة والخاصة طالما كانت تستخدم أساسا الحاسب الالكتروني في ممارسة أنشطتها سواء الاقتصادية منها أو الاجتماعية أو حتى السياسية والعسكرية، والملاحظ أنه يصعب في كثير من الأحيان تحديد نطاق ضحايا هذه الجرائم على نحو دقيق نظرا الى أنهم لا يعلمون شيئا عنها إلا بعد وقوعها، وفي هذه الحالة لا يحبذ أكثرهم الابلاغ عنها والتصريح بأن نظامهم المعلوماتي قد وقع عليه انتهاك بأي صورة كانت، وهذا السلوك السلبي يعتبر في حقيقة الأمر مغريا لمرتكبي جرائم المعلومات للاستمرار في نشاطهم الاجرامي[2]. وإن كان الأمر يجد ما يبرره بالنسبة للمؤسسات المصرفية، والشركات الكبرى التي تتعرض لأعمال النصب والاحتيال المعلوماتي، ومع ذلك تحجم عن التبليغ عنها تحت طائلة على عدم المساس

---

[1] - عبد الصبور عبد القوي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع: القاهرة، الطبعة الأولى، 2008، ص 58.

[2] - أنظر على التوالي: آمال قارة، الجريمة المعلوماتية، مذكرة لنيل درجة الماجستير في الحقوق، كلية الحقوق، جامعة بن عكنون، الجزائر، 2001، 2002، ص ص 27، 28/ عبد الصبور عبد القوي، مرجع سابق، ص 105.

بسمعتها لدى زبائنها وشركائها، لما في ذلك من خطورة على وضعها المالي، والخشية من عزوف الزبائن عن التعامل معها لعجزها عن توفير الحماية اللازمة لشبكاتها الداخلية والخارجية[1].

على صعيد آخر، فإن فئة الأطفال هم أكثر ضحايا جرائم المعلومات، والاحصائيات العالمية تشير إلى أن 80 ٪ من الأطفال الذين يستخدمون البريد الالكتروني يستقبلون رسائل بريد الكتروني دعائية كل يوم وبخاصة خلال فترات العطلة، حيث يقضي الكثير منهم الوقت في تصفح الانترنت، وغالبا ما يتم استدراج الأطفال عن طريق غرف الدردشة، وطلب صورهم للعبث بها ونشرها خصوصا بالنسبة لفئة الفتيات[2].

[1] - معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي وعلوم جنائية، جامعة باتنة، 2011، 2012، ص 17.

[2] - أنظر: سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، "الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهتها"، مجلة التقني، جامعة التعليم التقني، (العراق)، المجلد 24، العدد 9، 2011، ص 48.

المبحث الثاني

خصائص وسمات الجريمة المعلوماتية

كثيرا ما يقع الخلط وعدم التمييز بين خصائص الجريمة المعلوماتية وصعوبات مكافحتها، على الرغم من وجود حدود فاصلة بين الموضوعين، فخصائص الجريمة المعلوماتية يراد بها ما تنفرد به من مميزات، والتي لا يمكن فصلها بالضرورة عنها مقارنة بباقي الجرائم العادية الأخرى، في حين أن صعوبات مكافحة الجريمة المعلوماتية تشكل مجموعة من التحديات التي لا تتعلق بالجريمة المعلوماتية لوحدها، بل تشترك فها كذلك مع بعض الجرائم الأخرى العابرة للحدود أو الجرائم المنظمة، وهي ليست لصيقة بالجريمة المعلوماتية بالقدر الذي لا يمكن فصله عنها،

وعليه فإن مسألة صعوبة الاثبات، أو التحقيق في الجرائم المعلوماتية ليست سمات ملازمة للجريمة المعلوماتية، بقدر ما هي إشكاليات أو تحديات مرتبطة بالجريمة المعلوماتية، وسوف يأتي الحديث عنها لاحقا.

انطلاقا مما تقدم يمكن حصر خصائص الجريمة المعلوماتية على النحو التالي:

المطلب الأول: وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات

يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها الكترونيا، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها، أو طباعتها،

وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية[1].

وعلى الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الادخال، المعالجة، الاخراج)، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر الى طبيعتها ارتكابها الا في وقت محدد، ففي مرحلة الادخال المعلوماتي يمكن ادخال معلومات غير صحيحة، أو عدم ادخال وثائق أساسية، وفي هذه المرحلة، وفي مرحلة المعالجة الآلية للبيانات، فإنه يمكن إجراء أي تعديلات تحقق الهدف الاجرامي عن طريق التلاعب في برامج الحاسب الآلي، أما في مرحلة المخرجات فقد يقع التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخلت فيه وعالجها بطرقة صحيحة[2].

من المفيد الاشارة أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، ومن الشائع وصف بيانات الحاسوب مثلا كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب، توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر لم يحدد موقفه، لكن من المرجح في الممارسة العملية أن تتضمن تلك البيانات والمعلومات على

---

[1] - عادل يوسف عبد النبي الشكري، مرجع سابق، ص 115.

[2] - محمد ياسر أبو الفتوح، "خصائص وتصنيفات الجريمة المعلوماتية"، مقال منشور على الموقع الالكتروني (تاريخ الزيارة 2017/11/11):

Almohakmoonalarab.ahlamontada.com/109-topic

وللمزيد من التفاصيل حول خصوصية صور الإعتداء في مجال الجريمة المعلوماتية راجع:

محمد حماد مرهج الهيتي، مرجع سابق، ص 108.

وسائط التخزين المادية (مثل الأقراص الصلبة، وبطاقات الفلاش للتخزين)، وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية، أو تردد الراديو[1]

المطلب الثاني: الصبغة العالمية للجريمة المعلوماتية

تتصف الجريمة المعلوماتية بكونها جريمة ذات بعد عالمي أو دولي، لكن لا ينبغي أن يفهم من ذلك أنها جريمة دولية، ذلك أن هذه الأخيرة محددة على سبيل الحصر ومعرفة وفق نظام روما الأساسي في: جرائم الحرب، جرائم العدوان، جريمة الابادة البشرية، الجرائم ضد الانسانية، ما يجعل بالضرورة التفرقة تدق بين النوعين، فالجريمة المعلوماتية تصنف في مجال القانون الجنائي الدولي، بخلاف الجريمة الدولية التي تصنف في مجال القانون الدولي الجنائي[2].

---

[1] – ذياب موسى البداينة، "الجرائم الالكترونية (المفهوم والأسباب)"، ورقة علمية مقدمة الى الملتقى العلمي الموسوم ب: الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية، عمان الأردن، 2014.

[2] – ذلك أن الجريمة المعلوماتية سلوك غير مشروع كما سبق تبيان ذلك بحيث يمس مصالح خاصة أو عامة داخل حدود دولة معينة، مع امكانية تجاوز هذه الحدود الى دولة ثانية وثالثة أو أكثر من ذلك ما يجعلها عابرة للحدود، في حين أن الجريمة الدولية هي كل فعل أو سلوك مخالف لقواعد القانون الدولي يتضمن اعتداءا على القيم والمصالح الدولية يرتكبه شخص طبيعي واحد، أو مجموعة من الأشخاص سواء لحسابهم الخاص، أو لمصلحة دولة معينة، أو لمصلحة مجموعة من الدول، أو كانت بتحريض أو مساعدة منهم، مع الاشارة في هذا الصدد أن تجريم الأفعال المخالفة للقانون الدولي لم يأت صدفة، بل كان نتاج أحداث شهدتها الساحة الدولية ارتكبت في ظلها أفعال أخلت بالسلم، والأمن الدوليين، ومست بالحقوق الأساسية للإنسان ما جعل المجتمع الدولي يضفي عليها وصف الجرائم الدولية=========

والحديث عن صفة العالمية للجريمة المعلوماتية ارتبط بالتقنيات الحديثة، وما صاحبها من تطور في مجال الاتصال بحيث ألغى الحدود الجغرافية بين الدول، فتخطت بذلك الجريمة المعلوماتية حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى عدة بلدان على مستوى العالم، فالتقنيات المتصلة عالميا قد جعلت من هذه الجريمة عابرة للحدود، وعليه فالطبيعة العالمية تمكن الجاني من ارتكاب الجريمة في دولة ما، وتؤثر على المجني عليه في دولة أخرى[1]، بل أنه من الممكن أن يكون هناك ضرر محتمل في بلد ثالث، وعليه تعد جرائم المعلومات شكلا جديد من الجرائم العابرة للحدود الوطنية أو الاقليمية، أو القارية، وقد خلفت هاته الخاصية الكثير من الاشكالات القانونية في مسألة الاختصاص القضائي والتحديات التي تقترن به[2].

المطلب الثالث: الجريمة المعلوماتية أقل عنفا وجهدا في التنفيذ

لا تتطلب جرائم المعلومات عنفا لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون

= أنظر في هذا الصدد وتفاصيل أخرى في الموضوع على التوالي:

- محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2009/2008، ص 70.

- عصماني ليلى، التعاون الدولي لقمع الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي، جامعة وهران، 2013/2012، ص 12.

[1] – مشتاق طالب وهيب، مرجع سابق، ص 345.

[2] – راجع على التوالي: محمد علي سالم، مرجع سابق، ص 92./ محمد حماد مرهج الهيتي، مرجع سابق، ص ص 99، 100.

في صورة مماسة العنف والايذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع والكسر وغير ذلك.

وعلى هذا الأساس تتميز جرائم المعلومات بأنها من الجرائم الهادئة، أو الناعمة، حيث لا تحتاج الى العنف، وكل ما تحتاج إليه هو عامل الخبرة، والذكاء، والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في إرتكاب الأفعال غير المشروعة، فهي من الجرائم النظيفة التي تستخدم الأرقام والبيانات وليس لها أثر خارجي مادي[1].

---

[1] - أنظر في هذا الخصوص:

- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013، ص 16.

- طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات: الاسكندرية، 2016، ص 34.

- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، مرجع سابق، ص ص 27، 28.

الفصل الثاني

إشكالات مكافحة

الجريمـــة المعلـــوماتية

الفصل الثاني
إشكالات مكافحة الجريمة المعلوماتية

تعكف التشريعات الداخلية والدولية على البحث في كل مرة عن الحلول المجدية للتقليل من حدة النشاط الإجرامي لتنامي خطر انتشار الجرائم المعلوماتية إن لم نقل القضاء عليها بشكل تام، على الرغم من أن الكثير من المحاولات تعترضها العديد من الاشكالات الموضوعية والإجرائية، مما يؤكد خصوصية مكافحة الجريمة المعلوماتية مقارنة بغيرها من الجرائم التقليدية.

وسنحاول من خلال هذا الفصل التطرق لمختلف تلك الاشكالات في ضوء ما هو مستقر عليه في أغلب التشريعات المقارنة، لكن تقسيمنا المنهجي للإشكالات أو الصعوبات المرتبطة بالجرائم المعلوماتية لا ينبني على أساس ما هو موضوعي وآخر اجرائي، بل سوف يتم تناوله من خلال التركيز على الاشكالات المرتبطة بالقانون الواجب التطبيق على الجرائم المعلوماتية من جهة (المبحث الأول)، والإشكالات المرتبطة بخصوصية الاثبات والتحقيق في الجرائم المعلوماتية من جهة ثانية (المبحث الثاني).

المبحث الأول: الاشكالات المرتبطة بالقانون الواجب التطبيق على الجريمة المعلوماتية

الواقع أن مكافحة جرائم المعلومات كما أسلفنا يصطدم بعدة معوقات من أبرزها تحديد القانون الواجب التطبيق عليها من الناحيتين الموضوعية والإجرائية على اعتبار أنها من الجرائم العابرة للحدود الدولية، إذ غالبا ما ترتكب في إقليم دولة معينة ويكون ضحاياها في دولة أخرى، لذا تعد هذه الخاصية من أبرز السمات التي تميز الجرائم المعلوماتية.

وفي هذا الصدد من المتصور اليوم على سبيل المثال لا الحصر أن يتم اختراق كمبيوتر يوجد في بلد آخر أو إتلاف معطياته[1]، دون أن تكون الحدود الجغرافية حائلا أمام ذلك، طالما أن ذلك يتم في فضاء معلوماتي لا يعترف بالحدود، الأمر الذي يشكل تحديا كبيرا لمختلف الدول، لاسيما في ظل صعوبة تعقب مرتكبي هذه الجرائم بسبب عدة عوامل هي: مبدأ الشرعية الجنائية وعدم كفايته لاستيعاب صور النشاط الإجرامي المرتبط بهذا النوع من الجرائم،وإشكالية تنازع القوانين الجنائية المتعلقة بمكافحتها، فضلا على نقص التنسيق والتوظيف المجدي والكافي للآليات الدولية لمكافحة الجريمة الالكترونية، وسوف نتناول بشكل مستقل كل عامل على حدة:

[1] – سميرة معاشي، مرجع سابق، ص 281.

المطلب الأول: عدم كفاية مبدأ الشرعية الجزائية لاستيعاب كل صور النشاط الاجرامي المتعلق بالجريمة المعلوماتية

إن غالبية التشريعات الجنائية المقارنة تعتد بمبدأ الشرعية الجنائية[1]، وتعتبره من أبرز المبادئ التي تحكم التجريم والعقاب، وعلى الرغم من عدم وجود تعريف جامع مانع لمبدأ الشرعية الجنائية، غير أن ذلك لا يحول دون إيراد التعريف العام الفقهي المتفق عليه، والذي مفاده أن المقصود بالمبدأ هو حصر مصادر التجريم والعقاب في نصوص القانون. فتحديد النشاط، أو السلوك الذي يعد جريمة جزائية، وبيان أركانه، وكذلك تحديد العقوبات المقررة لها، سواء من حيث نوعها، أو مقدارها هو من اختصاص المشرع وحده، وما على القضاء إلا تطبيق ما يضعه المشرع من نصوص في هذا الشأن[2].

وبذلك يتبين أن مبدأ الشرعية الجزائية يرسم الحدود بين ما يعتبر في نظر المشرع الجنائي من سلوكات تخل بأمن الجماعة، ونظامها وسكينتها، فتكون لديه جديرة بالتجريم والعقاب، وبين السلوكات الأخرى التي لا تعتبر كذلك، فتظل أفعالا مباحة وغير مجرمة تطبيقا لقاعدة أن الأصل في الأشياء

---

[1] - ومن المفيد التنويه في هدا الصدد إلى أن بعض التشريعات المقارنة لم تأخذ بمبدأ الشرعية ولاسيما قانون العقوبات الألماني الصادر سنة 1935 وقانون العقوبات الدنماركي الصادر سنة 1933: علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت، 1982، ص 35، مشار إليه في: عادل يوسف عبد النبي الشكري، مرجع سابق، ص 120.

[2] - طه زاكي صافي، القواعد الجزائية العامة فقها واجتهادا،المؤسسة الحديثة للكتاب، طرابلس: لبنان،1997، ص 119.

الاباحة[1]، لكن رغم ذلك لا يخفى بأن المجتمع هو نفسه بحاجة لحماية خاصة من المجرمين الذين يقدمون على أفعال لم يلحظها المشرع، ولم يكن بإمكانه أن يتوقعها بالرغم من خطورتها، وتبعا لذلك وفي كل مرة يسهى عن بال المشرع تجريم بعض الأفعال، يدفع بالمجرمين، وتحت طائلة لا جريمة ولا عقوبة من دون نص إلى التلاعب بالقانون ناشرين الفساد والفوضى في المجتمع بكل فئاته، وحتى لو افترضنا تحرك المشرع، فإن تحركه سيأتي متأخرا[2].

ومهما يكن من أمر، يظل مبدأ الشرعية الجنائية مثارا للنقاش بين فقهاء القانون الجنائي، خاصة وأن الإشكال لم يعد ينصب اليوم حول تحديد الدلالة القانونية للمبدأ بقدر ما ينصب على مسألة عدم كفايته لاستيعاب صور النشاط الإجرامي للجريمة التي تمس بمصالح خاصة أو عامة، والإشكال يجد مجالا أوسع للنقاش في دائرة الجرائم التي تتم في الفضاء الإلكتروني، وذلك بالنظر إلى التطورات التكنولوجية المتلاحقة[3]، والتي واكبتها أفعال تضر بالأموال والأشخاص في الكثير من الأحيان، لكن عادة ما يفلت مرتكبوها من العقاب، على اعتبار أن القوانين الجنائية السارية المفعول لا تدخل تلك الأفعال في دائرة الجرائم، وذلك تطبيقا لمبدأ الشرعية الجنائية الذي يغل يد القضاة على توقيع العقوبات على هؤلاء حتى ولو اقتنع القاضي بخطورة الفعل.

وهكذا أضحى مبدأ الشرعية الجنائية حائلا أمام مواجهة الآثار السلبية للتطورات التكنولوجية التي يشهدها عالمنا المعاصر، ولا غرابة في ذلك طالما أن

---

[1] – عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام)، دار موفم للنشر، الجزائر، 2009، ص 95.

[2] – طه زاكي صافي، مرجع سابق، ص 121.

[3] – سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الله، مرجع سابق، ص 47.

المشرع عندما يقضي بتجريم بعض الأفعال ويحدد العقوبات المقررة لها إنما يأخذ بعين الاعتبار المصالح القائمة أثناء وضعه لها، وعلاوة على ذلك يكتفي بتحديد بعض صور الأفعال التي يمكن أن تضر بتلك المصالح وقت وضع القاعدة القانونية الجنائية، ولا شك في أن هذا الأمر ينطبق على الجرائم العادية والمعلوماتية حد سواء، الأمر الذي يجعل الأشخاص الذين يرتكبون الأفعال الخطيرة التي لا تدخل في نطاق الجرائم المنصوص عليها قانونا في منأى من أي متابعة جنائية[1].

لكن ما سبق لا ينبغي أن يفسر على أساس التمسك بإلغاء مبدأ الشرعية الجزائية من نطاق الجرائم الماسة بأنظمة المعلوماتية، ذلك أن هذا المبدأ يجب أن يبقى هو المحرك والدافع لأي حركة تجريم أو عقاب، ولو تعلق الأمر بالجرائم المستحدثة التي يصعب إن لم نقل يستحيل أن نرسم دائرة خطورتها، ونحدد تبعا لذلك نطاق السلوكات الاجرامية المتصلة بها، غاية ما في الأمر أن المشرع الجزائي إنما يتعامل مع جرائم غير محددة في الوسائل المستخدمة بشأنها وكذا دائرة خطورتها ما يؤكد فرضية أنه يهدف إلى حماية مصالح ليست مستقرة وثابتة الخطورة[2]، ولما كان مبدأ الشرعية الجزائية يضع قيودا بالنسبة

---

[1]– وهو ما حصل فعلا بالفلبين عام 2000 عندما قبضت الشرطة على شاب وفتاة بتهمة نشر فيروس، إلا أنه أطلق سراحهما فيما بعد لعدم وجود نص قانوني يجرم هدا الفعل في القانون الفليبيني: القاضي فاضل عباس الملا، "الخطورة الأمنية للجرائم الإلكترونية وسبل مكافحتها"، مجلة كلية الجامعة الإسلامية، العدد 7، النجف العراق، 2009، ص 178.

[2]– يمكن تحديد السبب في ذلك أن جرائم المعلومات تختلف اختلافا كبيرا عن الجرائم التقليدية الأخرى، ومناط هذا الاختلاف يتمثل في أن الجرائم التقليدية على غرار جرائم الأشخاص والأموال تتقاطع جميعها في حماية مصالح ومعطيات مادية تتم في فضاء مادي.=

للقاضي الجزائي الذي لا يملك أن يتوسع في تفسير النص الجزائي، أو يلجأ إلى القياس، كان من واجب المشرع الجزائي وهو يسن النصوص الجزائية الموضوعية المتعلقة بمجال المعلوماتية أن يدقق في إختيار العبارات الدالة على حدود ونطاق السلوك الاجرامي على نحو يستوعب بشكل دقيق الوقائع التي تهدد أو تمس بالمصالح القائمة محل الحماية، وكذا العقوبات المتناسبة معها.

ومن ناحية أخرى وجب عليه أن يراعي ما قد يستجد من تهديد أو إضرار لتلك المصالح، وهو أمر يرتبط بالضرورة بالتطور الحاصل على مستوى التقنيات التكنولوجية المستخدمة في ارتكاب جرائم المعلومات، بحيث يسمح ذلك بالاستيعاب الآلي للنصوص الجزائية لكل ما قد يطرأ من مستجدات، مما يجنب المشرع العقابي التعديل المستمر والمتتالي وحتى المتأخر لجرائم المعلومات.

إن التسليم بالطرح السابق يؤدي فضلا على تدارك المشرع الجزائي في التزامه بمبدأ الشرعية الجزائية لحدود الوقائع التي تشكل جرائم معلوماتية بشكل مستمر، إلى توسيع نطاق الحماية الجزائية للبيانات والمعطيات، بل وحتى للنظام المعلوماتي برمته، وهذا من أجل ضمان عدم إفلات المجرم المعلوماتي من الكثير من مظاهر السلوك الاجرامي الذي يقترفه تحت طائلة التطور الحاصل على مستوى أنظمة المعلوماتية، والذي يرافقه في الوقت ذاته تطويع وسائل ارتكاب الجرم المعلوماتي مع تلك الأنظمة.

= الأمر الذي يحسن أن نطبق عليها وسائل التحقيق والاثبات المعمول بها، بخلاف جرائم المعلومات التي تنصب على معطيات ومصالح مفترضة تتم في فضاء سبيراني غير مادي، الأمر الذي يصعب معه إعمال الوسائل التقليدية المتبعة بشأن الجرائم العادية، وهذا الأمر يؤدي بحكم اللزوم القانوني إلى ضرورة استقلال جرائم المعلومات بقانون موضوعي وآخر اجرائي يتفق وخصوصيتها كجرائم مفترضة.

المطلب الثاني: إشكالية تنازع القوانين الجنائية المختصة بمكافحة الجريمة المعلوماتية

من المعلوم أن جرائم المعلومات تتميز بخاصية العالمية[1]، إذ تعد من الجرائم العابرة للحدود، الأمر الذي يثير إشكالا قانونيا يتعلق بالقانون الواجب التطبيق على الجريمة المرتكبة في بيئة رقمية، وما إذا كان القاضي يحتكم إلى قانون الدولة التي أرتكب الفعل المجرم على إقليمها أم قانون الدولة أو الدول التي حصل الضرر على إقليمها[2].

لذا تقف صفة العالمية التي تصطبغ بها الجريمة المعلوماتية حاجزا أمام إمكانية متابعة مرتكبيها[3]، على إعتبار أنه يؤدي إلى صعوبة تحديد القانون الواجب التطبيق على تلك الجرائم، وبالتالي تعجز قواعد الاختصاص التقليدية عن إيجاد حلول للمسألة حتى وإن طبقت[4]، طالما أن التنازع يحصل بين أكثر من تشريعين لمواجهة الفعل الإجرامي نفسه[5].

---

1 – See : European Crime Prevention Network, Cybercrime: **A theoretical overview of the growing digital threat**, EUCPN Secretariat, February 2016, Brussels, p.11, available at: eucpn.org/sites/default/files/.../theoretical_paper_cybercrime_.pdf, Date of access; 15 January 2017.

2 – للمزيد من التفاصيل بشأن الموضوع أنظر: صفاء حسن نصيف، "التحديات الإجرائية المتصلة بالجرائم المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة بغداد، المجلد الخامس، العدد الثاني، 2016، ص 274.

3 – سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الله، المرجع السابق، ص 50.

4 – راجع في هذا المعنى: رصاع فتيحة، مرجع سابق، ص 43.

5 – ميسون خلف حمد الحمداني، "مشروعية الأدلة الإلكترونية في الإثبات الجنائي"، مجلة كلية الحقوق، جامعة النهرين، العراق، العدد 2، المجلد 18، 2016، ص 226.

وفي السياق نفسه تثار مسألة تنازع الاختصاص القضائي بالنظر في بجريمة معلوماتية معينة[1]، وفي هذا الصدد يضرب البعض مثلا بالجريمة التي ترتكب من طرف أجنبي على إقليم دولة ما، حيث يعود الاختصاص القضائي في هذا الفرض إلى الدولة التي أرتكب الفعل المجرم على إقليمها تطبيقا لمبدأ الإقليمية، كما يعود أيضا إلى الدولة التي يحمل الجاني جنسيتها تطبيقا لمبدأ الاختصاص الشخصي.

علاوة على ذلك من المتصور أن يحصل تنازع الاختصاص القضائي في حالة ارتكاب الجريمة من طرف أحد المواطنين على إقليم الدولة التي يتبعها، وحصول الضرر على إقليم دولة أخرى، إذ وفقا لمبدأ الاختصاص الإقليمي يؤول اختصاص النظر في النزاع إلى قضاء الدولتين دون مفاضلة بينهما.

ومن ثم، فإن الجريمة المعلوماتية ومن حيث المبدأ تبقى خارج أي سيطرة أو رقابة من أي جهة، بحيث لا يمكن القول بخضوعها لاختصاص قانون جنائي معين، مما يثير حتما إشكالية تحديد القانون الواجب التطبيق على هذه الجرائم، آخذين بالاعتبار إجماع الدول على إعطاء قانونها الوطني الاختصاص، إذا امتدت آثار السلوك الاجرامي إلى إقليمها، أو مست بالمصالح الأساسية في تلك الدول[2].

لكن هذا الأمر يتلاشى أمام إختلاف المفاهيم المتعلقة بالجرائم المعلوماتية بين الدول ذلك أن جميع الأنظمة في العالم تعتبر أن الأفعال غير المشروعة المرتبطة بالمعلوماتية جرائم معاقب عليها، لكنها تختلف من حيث نطاق تطبيق

1 - Marc D. Goodman and Susan W. Brenner, **Why the Police don't care about computer crime**, Harvard Journal of Law & Technology , Volume 10, Number 3 Summer 1997.

2 – صفاء حسن نصيف، مرجع سابق، ص 277.

هذا التجريم، يفهم من ذلك أن أفعالا معينة يمكن أن تبقى خارج دائرة هذا الوصف، إذا لم يوجد نص يؤكد صراحة على شمولها، فرغم تزايد خطر جرائم المعلومات على الأشخاص والأموال، والمصلحة العامة إلا أن بعض الدول لم تدرج بعض الأفعال الماسة بالنظام المعلوماتي في دائرة التجريم[1].

ومهما يكن من أمر فقد اقترح الفقه حلولا عاجلة لمواجهة مشكل تنازع الاختصاص القضائي بالنظر في الجرائم المعلوماتية، ومن جملة تلك الحلول، ضرورة تدخل التنظيم القانوني الدولي في موضوع تحديد الاختصاص دون ترك الأمر للتنظيم القانوني الداخلي، فمن الطبيعي أن تلجأ كل دولة الى إعطاء قوانينها الاختصاص في نظر هذه الجرائم اذا مست مصالحها مما يفاقم من مشكلة تحديد الاختصاص خاصة وأن الجرائم لا تتقيد بحدود فيزيائية معينة،وعليه يتعين التفرقة في تحديد الاختصاص في الجرائم المعلوماتية حسب جانب من الفقه الجنائي تبعا للمصالح التي يقع الاعتداء عليها، فكلما كانت هذه المصالح تهم الجماعة الدولية بشكل عام، ومحل إجماع على تجريمها من قبلها عقد فيها الاختصاص لقانون أي دولة يتم فيها ضبط الجريمة كمحل النشاط الاجرامي أو محل تحقق الآثار، أو يتم فيها ضبط الجاني على أساس مبدأ الاختصاص العالمي على غرار بعض الجرائم التقليدية التي يثبت فيها للدول مثل هذا الاختصاص، وفي حال مست هذه الجرائم مصالح دولة بعينها دون غيرها،أو مست مصالحها الحيوية على نحو ينبئ بمخاطر كبيرة كالهجمات

---

[1] - شوقي يعيش تمام، شبري عزيزة، "تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية"، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة بسكرة، عدد 15، سبتمبر 2017، ص 99.

الالكترونية على المواقع الحكومية الحساسة، وغيرها فقد أعطي قانون تلك الدولة الاختصاص للنظر في مثل هذه الجرائم.

أما فيما يتعلق بالجرائم الأخرى التي تقع على مصالح متعددة خارج الحالات السابقة، أين تتعدد فيها أماكن تحقق آثار الجريمة أو تنازع فيها الاختصاص بشكل عام، فمن الممكن اللجوء إلى فكرة الاختصاص الأصلي، والاختصاص الاحتياطي أو الثانوي الذي يلجأ إليه في حال تعذر الأخذ بقانون الاختصاص الأصلي وفقا لقواعد يتم الاتفاق عليها في ضوء الاتفاقية المقترحة بهذا الشأن[1].

وفي جميع الأحوال تعتبر مسألة تنازع القوانين وتنازع الاختصاص القضائي من أبرز المعوقات التي تحول دون مكافحة الجرائم المعلوماتية، لا سيما في ظل عجز قواعد الاختصاص التقليدية عن حل المسألة، ولا غرابة في دلك طالما أن تلك القواعد وضعت أصلا لمعالجة حالات التنازع التي تحصل بخصوص أفعال محددة واقعيا وليس افتراضيا، وهو الأمر الذي دفع بالقضاء نحو طرح معايير اختصاص بديلة تتلاءم مع الطبيعة الخالصة للجريمة الإلكترونية، وليس أدل على ذلك ما أقره القضاء الفرنسي عندما بين أن الاختصاص في جرائم الصحافة الإلكترونية يؤول إلى محل تمركز الموقع الذي نشرت الأقوال أو المعلومات بواسطته، وعلاوة على ذلك تختص الجهة القضائية التي يقع في دائرتها المكان الذي ارتكب فيه التقليد أو مكان نشره بنظر جرائم التقليد

[1] – صفاء حسن نصيف، مرجع سابق، ص 278.

المرتبطة بحقوق الملكية الفكرية[1].

إن الحل المناسب من وجهة نظرنا لتجاوز عقبة تنازع الاختصاص يتمثل في التسليم التدريجي بتطبيق مبدأ عالمية النص الجنائي،وهو أمر يقتضي التقاء إرادة الدول حول إطار إتفاقي مشترك يحدد القواعد الموضوعية التي تحكم مادة الجريمة المعلوماتية، ويرسم في الوقت ذاته الضوابط الاجرائية المتبعة في ملاحقة المجرم المعلوماتي والتحقيق معه، تمهيدا لتقديمه للمحاكمة.

المطلب الثالث: ضعف التنسيق
والتعاون الدولي لمكافحة الجريمة المعلوماتية

على الرغم من الخطورة التي تكتسيها جرائم المعلومات، إلا أن التنسيق والتعاون الدوليين بشأنها لم يبلغ درجة الاهتمام الذي تشهده بعض الجرائم الدولية على غرار الجرائم الإرهابية، لذا يكون من الأهمية بمكان توسيع نطاق هذا التنسيق والتعاون إلى جميع الجرائم التي تهدد المصلحة العامة والأشخاص والأموال، بما فيها الجرائم المعلوماتية، من خلال ربط اتفاقيات تعاون بين الدول، بما يتيح إمكانية تقديم طلب إلى سلطات الدولة المعنية من أجل تزويدهم بالمعلومات والأدلة في مرحلتي التحري والتحقيق.

فإذا كانت الجريمة المعلوماتية تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، فإن ذلك يبرز أهمية إمتهان قواعد الاختصاص والقانون الواجب التطبيق، فيما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه

---

[1] – يوسف قجاج، "الجريمة الإلكترونية وإشكالية القواعد الإجرائية"، منشور بالموقع: http://www.alkanounia.com، تاريخ الإطلاع 02 جانفي 2017.

الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها، وما تثيره من مشكلات في مجال الاختصاص القضائي، مع ملاحظة أن هذا الإشكال يتفاقم أكثر في ظل امتداد الملاحقة والتحري والضبط والتفتيش خارج الحدود[1]، الأمر الذي يتطلب وجود تعاون دولي يكفل مكافحة الجريمة الإلكترونية من جهة، ولا ينتهك مبدأ سيادة الدول على إقليمها من جهة ثانية.

والواقع أن خاصية العالمية التي تميز جرائم المعلوماتية قد دفعت رجال القانون والفقهاء إلى الدعوة لمواجهتها من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد من شأنه تدارك النقائص والثغرات التي تعتري منظومة القوانين الداخلية للدول وذلك بهدف التقليل من حدة آثار هذه الجريمة.[2]

وفي هذا الإطار تظافرت الجهود من أجل وضع إطار قانوني اتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية ومعاقبتهم، وهو الأمر الذي تجسد في إتفاقيات ثنائية ومتعددة الأطراف متعلقة بالمسألة، سواء على المستويين الدولي أو الإقليمي.

فمن المعلوم أن الجرائم المعلوماتية ظهرت في الدول المتقدمة، ولا غرابة في ذلك على اعتبار أن تلك الدول كانت سباقة إلى استخدام البيئة الرقمية في تعاملاتها العادية والتجارية والمالية وغيرها[3].

---

[1] – ألتريش سايبر، "جرائم الكومبيوتر والجرائم الأخرى في مجال المعلومات"، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، ترجمة سامي الشوي، دار النهضة العربية، القاهرة، مصر، 1993، ص 58.

[2] – شوقي يعيش تمام، شبري عزيزة، مرجع سابق، ص 95.

[3] – ذلك أن خطر الجريمة المعلوماتية يمس جميع الميادين، فمن المتصور أن تتسبب في خلق شلل كامل للأنظمة المدنية والعسكرية والأرضية والفضائية، وتعديل المعدات الإلكترونية،=

لذا برزت الحاجة إلى توحيد الجهود الدولية في هذا المجال، وهو ما تجسد فعلا بعقد الكثير من المؤتمرات المتعلقة بالموضوع وإبرام اتفاقيات تخص المسألة، وعلاوة على ذلك تم وضع قوانين نموذجية لمواجهة هذه الجرائم في مجالات متعددة، ومن أجل بيان تلك الجهود من الأهمية بمكان الإشارة إلى بعضها بإيجاز فيما يأتي[1]:

أ- المؤتمر الدولي لحقوق الإنسان الخاص لسنة 1968:[2]

يعتبر هذا المؤتمر من أول المؤتمرات التي تعكس الجهود الدولية في مكافحة جرائم الأنترنيت، حيث عقد بالعاصمة الإيرانية في نهاية ستينيات القرن الماضي، وقد أكدت الفقرة 18 من هذا الإعلان صراحة إلى أن التقدم العلمي

=واختراق النظم المصرفية، وإرباك حركة النقل وشل محطات الطاقة بواسطة قنابل معلوماتية ترسلها على مسافات تتعدى آلاف الأميال، مشار إليه: أحمد عبد الرحمان البعادي، "دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، أيام 23 و24 و25 سبتمبر 2012، الخرطوم، السودان، ص 03.

[1] – راجع: سيناء عبدالله محسن، "المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية"، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم في الدول العربية POGAR -UNDP ، يومي 19 و20 يونيو 2007، المملكة المغربية، ص 54 وما بعدها.

[2] – **La proclamation de Téhéran**, L'acte final de la Conférence internationale des droits de l'homme, Téhéran, du 22 avril au 13 mai 1968, U.N. Doc. A/CONF. 32/41 à 3 (1968), disponible sur le site: www1.umn.edu, en date du 15 mai 2015.

والتقني يمكن أن يعرض حقوق وحريات الفرد للخطر[1]، وهو الأمر الذي لقي صدى واسعا من طرف الغالبية العظمى من الدول المتقدمة، وذلك من خلال التجسيد الفعلي لمضمون هذه التوصية في تشريعاتها الداخلية.

ب- قانون الأونسيترال النموذجي للتجارة الإلكترونية لسنة 1996:[2]

علاوة عن المؤتمر السابق الإشارة إليه، يعد هذا القانون من أهم الجهود الدولية في مجال مكافحة الجرائم المتعلقة بالمعلوماتية على المستوى الدولي، وقد كان لبنة للعمل الكبير الذي قامت به "الأنسترال" في سبيل وضع نصوص نموذجية لتزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية لمواجهة جرائم المعلوماتية في مجال التجارة الإلكترونية، وقد لقي هذا القانون قبولا من طرف مشرعي الدول والمتعاملين، لاسيما بعد أن إعتمدته لجنة الأمم المتحدة سنة 1996.

ج- القانون النموذجي المتعلق بالتوقيع الإلكتروني لسنة 2001:[3]

يعتبر هذا القانون تكملة للجهود التي بذلتها لجنة "الأونسترال" في سبيل مكافحة الجرائم المعلوماتية المتعلقة بالتجارة الدولية، حيث تكفل بوضع قواعد

---

1 - Le 18 alinéa de la proclamation de Téhéran dit que: « Si les découvertes scientifiques et l'évolution de la technique ont récemment ouvert dévastes perspectives au développement économique, social et culturel, ces progrès peuvent néanmoins mettre en danger les droits et libertés de l'individu et requièrent donc une attention vigilante ».Ibid.

2 – Loi type de la CNUDCI sur le commerce électronique (1996), disponible sur le site: https://www.uncitral.org/pdf/french/texts/.../05-89451_Ebook.pdf, en date du 04 mai 2015.

3 – Loi type de la CNUDCI sur les signatures électroniques (2001), disponible sur le site:https://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf, en date du 22 avril 2015.

موحدة من شأنها حماية التوقيع الإلكتروني، وهو ما كرسته الكثير من الدول في تشريعاتها الداخلية.

علاوة عن الجهود الدولية لمواجهة الجرائم المعلوماتية عكفت الكثير من الدول إلى معالجة هذه الجرائم على المستوى الإقليمي، وهذا ما يتضح من خلال النموذجين التاليين:

أ- الاتفاقية الأوروبية لجرائم الانترنيت لسنة 2001:

دخلت هذه الاتفاقية حيز التنفيذ سنة 2004، ويطلق عليها البعض تسمية اتفاقية بودابست، وقد جاءت تتويجا للجهود التي بذلها المجلس الأوروبي في سبيل التوصل إلى وضع إطار اتفاقي فعال لمكافحة الجرائم المعلوماتية، ومن أهم الدول التي وقعت عليها خارج دول الاتحاد الأوروبي نذكر جنوب إفريقيا واليابان والولايات المتحدة الأمريكية[1].

وتأتي أهمية هذه الاتفاقية في كونها اتفاقية تهدف إلى توفير إطار دولي مشترك للتعامل مع الجرائم الالكترونية حيث تلتزم الدول الموقعة عليها بتعديل تشريعاتها لمواجهة التحديات التي تفرضها تكنولوجيا المعلومات، إذ تولت تحديد الجرائم المعلوماتية، واعتماد أدوات إجرائية لمكافحة الجريمة المعلوماتية وضبط مرتكبيها[2].

وتتكون الاتفاقية من 44 مادة موزعة على عدد من الأبواب، بحيث جاء الباب الأول منها محددا للتعريفات وضبط المصطلحات، أما الباب الثاني فخصص

---

[1] – أحمد عبد الرحمان البعادي، مرجع السابق، ص 12.

[2] – Conseil de l'Europe, Convention sur la cybercriminalité, STE n° 185, Budapest, 23.XI.2001, pp.1-26, disponible sur le site:http://www.aedh.eu/, en date du 01 mars 2016.

للحديث عن التدابير الواجب إتخاذها على الصعيد الوطني، والباب الثالث يتعلق بالولاية القضائية والتعاون الدولي، والباب الرابع يتضمن الأحكام الختامية[1]

ب- قانون عربي استرشادي لمكافحة الجريمة المعلوماتية:

تم اعتماد مشروع هذا القانون في الدورة التاسعة عشر لمجلس وزراء العدل العرب سنة 2003، قبل أن يعتمده وزراء الداخلية العرب سنة 2004[2].

والملاحظ أن هذا القانون أشار لأنواع الجرائم التي تقع عن طريق الكمبيوتر والانترنت بصفة عامة، وأحال إلى التشريعات الداخلية كلما يتعلق الأمر بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها، وفي هذا السياق تضمن الباب السابع من هذا القانون فصلا خاصا يتعلق بالجرائم المعلوماتية الواقعة على حقوق الأشخاص، حيث أدرجت فيه أربعة مواد (من المادة461إلى المادة 464 منه)، وأشارت إلى حماية خصوصية الأشخاص من خطر الجرائم المعلوماتية وكيفية تتبع المجرمين والعقوبات المقررة لهذه الجرائم[3].

[1]- راجع الملحق المتعلق بالنص الكامل لاتفاقية بودابست لسنة 2001.

[2]- قشقوش هدى حامد، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، ص ص 102 وما بعدها.

[3]- تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته"، رسالة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ص 175.

رغم ذلك يبقى هذا القانون فضفاض ولم يعط الجريمة المعلوماتية ما تستحقه من الاهتمام[1] الأمر الذي جعل أحكامه عاجزة عن مواجهة خطر الجرائم المعلوماتية.

الجدير بالإشارة أن الاهتمام على المستوى المحلي بمكافحة الجريمة المعلوماتية قد زاد مع استشعار دول الجوار خطر الارهاب الدولي وفي هذا السياق اجتمع في ماي 2002 وزراء دول الثمانية بمدينة ترومبلن بكندا لاصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدود من أجل مكافحة الأعمال الارهابية، وفي ماي 2004 أصدرت دول الثمانية بيانا مشترك صدر بعنوان "مواصلة تعزيز القوانين المحلية"، وأوصى جميع الدول أن تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الالكترونية، والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالإنترنت[2].

ولعل أفضل وأنسب أنواع التعاون هو التعاون الثنائي الذي ساعد ومن المنتظر أن يضل محافظا على تلك الصفة في مكافحة الجريمة الالكترونية[3].

---

[1]- حسن بن أحمد الشهري، "قانون دولي موحد لمكافحة الجرائم الإلكترونية"، الملتقى الدولي الأول حول التنظيم القانوني للأنترنت والجريمة الالكترونية، المنظم من طرف كلية الحقوق والعلوم السياسية، يومي 27 و28 أفريل 2009، جامعة الجلفة، ص 40.

[2]- محمد سيد سلطان، مرجع سابق، ص ص 46، 47.

[3]- ومن أمثلة صور التعاون الثنائي في هذا الصدد ما حصل سنة 2000 عندما تم شن هجوم الكتروني على الشركات والأفراد في جميع أنحاء العالم بواسطة فيروس "I LOVE YOU" والذي تسبب في خسائر فادحة، فقام المركز القومي الأمريكي بالتحقيق في الحادث، وتم التعرف على المشتبه من خلال تعقب موقع الهجوم، وتم التعاون بين مكتب التحقيقات الفديرالي، ومكتب=

المبحث الثاني: الاشكالات المرتبطة بخصوصية الإثبات والتحقيق في الجريمة المعلوماتية

من المسلم به اليوم لدى فقهاء القانون الجنائي أن فلسفة التجريم والعقاب التي طبقت لفترات طويلة على الجرائم العادية لم تعد لها القدرة على مواجهة التحديات التي أحدثتها البيئة الإلكترونية، على اعتبار أن الجرائم الإلكترونية ترتبط بفضاء افتراضي غير واقعي، ولم يتوقف الأمر عند هذا الحد، بل أضحت معه حتى القواعد الإجرائية التقليدية عاجزة عن ضبطها، وقد طرح هذا النوع من الجرائم إشكالات حقيقية تتعلق بصعوبة معاينة مسرح الجريمة الإلكترونية، الأمر الذي أدى إلى عدم إمكانية جمع أدلة كافية عنها خاصة مع وجود ما يعرف بالدليل الرقمي (المطلب الأول)، فضلا عن صعوبة ملاحقة مرتكبيها والقبض عليهم في اطار عملية التحقيق في الجريمة المعلوماتية (المطلب الثاني).

المطلب الأول: إشكالية الاثبات بالدليل الرقمي

تثير جرائم المعلومات إشكالاً خاصا يتعلق بمسألة إثباتها، فلا يزال هذا الموضوع مجالاً خصباً للنقاش والتحليل من لدن رجال القضاء والقانون على السواء[1]، وقد برزت أهمية موضوع دليل الإثبات الإلكتروني للجريمة المعلوماتية بفعل قصور وسائل الإثبات الإجرائية المعمول بها في دائرة الجرائم العادية

= التحقيقات الوطني الفليبيني، وتم تحديد المشتبه فيه، والقبض عليه فيما بعد/ أنظر في هذا الصدد: محمد سيد سلطان، مرجع سابق، ص 49.

[1] – ميسون خلف حمد الحمداني، المرجع السابق، ص 209.

التي تتم في البيئة المادية، عن إثبات الجرائم التي ترتكب في البيئة الافتراضية[1].

من المفيد التنويه في هذا الإطار إلى أن مواجهة إشكالية إثبات الجريمة المعلوماتية أصبح يتطلب تضافر جهود القانونيين وأجهزة البحث والتحري على المستويين الوطني والدولي، فإذا كان لا يتعذر في الكثير من الأحيان الوصول إلى الدليل المادي بشأن الجرائم العادية فإنه من الصعوبة بمكان إثباته فيما يخص الجريمة المعلوماتية، لاسيما في ظل التطورات التكنولوجية التي يشهدها عالمنا المعاصر، والتي ساعدت على ارتكاب هذه الجرائم دون ترك أي دليل مادي يمكن أجهزة الضبط والتحري من متابعة مرتكبيها باستخدام الوسائل الإجرائية العادية[2]، ولا غرابة في ذلك طالما أنه يرتكبها مجرم يستفيد من الأساليب والتقنيات التكنولوجية الحديثة لتنفيذ الأعمال الاجرامية في مختلف أنحاء العالم عبر شبكة الانترنت، فضلا عن استخدامه ذكاءه وإمكانياته العلمية والعملية التي تمكنه من محو الآثار التي يمكن التعرف عليهم من خلالها[3].

ومهما يكن من أمر يبقى الدليل الرقمي هو المعول عليه في إثبات ارتكاب جريمة معلوماتية معينة في زمان ومكان محددين، لهذا يكون من الضروري علينا ضبط مدلوله والصعوبات المرتبطة به، فضلا على قيمته في الاثبات.

---

[1]- طالب جواد عباس، عبد الجبار ضاحي عواد، المرجع السابق، ص 62.

[2]- رصاع فتيحة، المرجع السابق، ص 44.

[3]- راجع في هذا الصدد كل من: برهان عزيزي، إثبات الجريمة في أحكام مجلة الاجراءات الجزائية، منشورات مجمع الأطرش للكتاب المختص: تونس، 2013،ص 200./ محمود وهيب، "ظاهرة العولمة وانعكاساتها الأمنية"، مجلة الأمن العام، المجلة العربية لعلوم الشرطة، العدد 164، القاهرة، مطابع الشرطة، يناير 1999، ص ص70- 71.

1- مدلول الدليل الرقمي والصعوبات المقترنة به:

تنوعت وتعددت التعاريف التي قيلت بشأن الدليل الرقمي، وتباينت بين التوسع في مفهومه والتضييق فيه، فقد عرفته المنظمة العالمية لدليل الكمبيوتر في أكتوبر 2001 بأنه المعلومات ذات القيمة المحتملة، والمخزنة،أو المنقولة في صورة رقمية، كما عرفه البعض الآخر على أنه الدليل المأخوذ من أجهزة الحاسب الآلي يكون في شكل مجلات أو نبضات مغناطيسية أو كهربائية، بحيث يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن التمسك به أمام القضاء[1].

يتبين لنا من خلال التعاريف السابقة أن الدليل الرقمي يختلف كثيرا عن نظيره المادي، فهو لا يرتبط بالضرورة بمسرح الجريمة، بل يستخلص من الوسيلة التي يشتغل بها النظام المعلوماتي، فهو يوجد حتى قبل حصول واقعة اجرامية في مجال النظام المعلوماتي، ولكن هذا لا يفسر سهولة الحصول عليه، أو الاحتجاج به في أي وقت، ذلك أن ما سبق ينقلب كعائق حقيقي أمام جهات التحقيق والقاضي الجزائي.

هذا ما يكشف عن وجود صعوبات حقيقية تتعلق بالدليل الرقمي في حد ذاته، وتتألف من البنية التي يستمد منها الدليل الرقمي وجوده، والتي تقوم على أساس المعلومات التي تتحرك وتنساب عبر الحواسيب الآلية والشبكات في شكل نبضات الكترونية غير مرئية مما يكسب الدليل ميزة التخفي، وغالبا ما

---

[1]- محمد بن فردية، "الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي، دراسة مقارنة"، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، السنة الخامسة، المجلد 09، العدد 01، 2014، ص 283.

تكون هذه المعلومات مشفرة مما يصعب من مسألة الوصول اليها خاصة إذا كانت معلومات خاصة أو خطيرة، وعلى الرغم من إعتماد بعض المؤسسات ذات الأنظمة المعلوماتية في حماية هذه الأنظمة عن طريق التشفير إلا أن بعض المجرمين المتخصصين يتمكنون من إختراق هذه الأنظمة، وبالتالي تصبح حمايتها غير جدوى سيما إذا كانوا من العاملين داخل المؤسسة[1].

وإن كنا لا ننكر من جهة أخرى ما يسجل للدليل الرقمي من قابليته للنسخ حيث أن من شأن ذلك التقليل أو بالأحرى اعدام مخاطر اتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الانشاء، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من التلف عن طريق نسخ طبق الأصل من الدليل[2].

وإزاء البحث عن الدليل الرقمي يستعين المختصون بمجموعة من الأدوات المادية، وبرامج التقاط الدليل الالكتروني، ومن أشهرها على الاطلاق برامج التتبع ونظام كشف الاختراق[3].

---

[1]– صفاء حسن نصيف، مرجع سابق، ص 261.

[2]– محمد بن فردية، مرجع سابق، ص 283.

[3]– يتمثل دور برامج التتبع في التعرف على محاولات الاختراق وتقديم بيان شامل عنها الى المستخدم الذي يتم اختراق جهازه ومثاله برنامج Hack tracer، وهو مصمم للعمل في الأجهزة المكتبية، وعندما يتم رصد محاولة للاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتفاء أثر مرتكب عملية الاختراق حتى يصل الى الجهاز الذي حدثت منه العملية، أما بالنسبة لبرنامج كشف الاختراق والذي يرمز له ب: IDS، فيقوم على أساس مراقبة بعض العمليات التي تتم على مستوى الشبكة أو الحاسب، مع تحليلها بحثا عن وجود أي اشارة تدل على وجود تهديد، حيث أنه يسجل الأحداث فور وقوعها، ويقارن نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، وفي حالة=

2- القيمة القانونية للدليل الرقمي في الاثبات:

إن المبدأ الذي يحكم حرية الاثبات في المسائل الجنائية والذي بمقتضاه يقدر القاضي قيمة الأدلة بحرية من دون أن يملي عليه المشرع أي حجية معينة لإعمالها مع خضوع هذا التقدير دائما للعقل والمنطق[1] لا يمكن تعميمه على إثبات الجريمة المعلوماتية المحكومة مسبقا وحتما بالدليل الرقمي، وهذا الأمر نابع بدوره من إختلاف البيئة التي يستخلص منها الدليل الجنائي، ففي الجرائم التقليدية المرتكبة في نطاق البيئة المادية يمكن الاستناد إلى أي وسيلة أو دليل إثبات من شأنه تكوين قناعة القاضي الجزائي، ولكن هذا لا ينطبق على جرائم المعلومات التي ترتكب في بيئة افتراضية، يكون محلها بيانات ومعطيات إلكترونية، ومن هنا انقسم الفقه بصدد مسألة قيمة الدليل الرقمي في الاثبات، وموقف القاضي الجزائي منه.

حيث يرى بعض الباحثين ضرورة إعطاء الدليل الالكتروني دلالة قانونية قاطعة ويدعوا الى اعتماده من قبل المحكمة كدليل كاف لا ثبات الادانة أو البراءة، ولو جاء مفردا من غير أدلة أخرى تدعمه، ويبرر أصحاب هذا الرأي موقفهم بصعوبة استخلاص الأدلة في البيئة الرقمية من جهة، ونقص الكوادر المتخصصة، وانخفاض كفاءتها من جهة أخرى، فضلا على أن القول بخلاف ذلك يؤدي الى افلات الكثير من الجناة.

= اكتشافه لإحدى هذه الصفات يقوم بإنذار مدير النظام، ويسجل البيانات الخاصة بذلك الاعتداء، أنظر في هذا الخصوص: بن فردية محمد، مرجع، ص 285.

[1] – عبد الله بن صالح بن رشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الاثبات بين الشريعة والقانون وتطبيقاتها في المملكة السعودية، مذكرة ماجستير في العدالة الجنائية، أكاديمية نايف للعلوم الأمنية، كلية الدراسات العليا، ص 77.

في حين يفرق رأي آخر بين فرضين، الأول هو القيمة القانونية القاطعة للدليل، والثاني هو الظروف والملابسات التي وجد فيها الدليل، فتقدير القاضي لا يتناول الفرض الأول لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا مجال للقاضي في مناقشة الحقائق العلمية، أما الظروف والملابسات التي وجد فيها هذا الدليل فهي تدخل في نطاق السلطة التقديرية بحيث يمكن أن يستبعد هذا الدليل رغم قطعيته عندما يلاحظ القاضي أن وجوده لا يستقيم مع ظروف الواقعة وملابساتها[1].

وتبعا لهذا الطرح يكون الدليل الرقمي باطلا اذا تم الحصول عليه بطريق مخالف لما يقضي به القانون، ولهذا الأمر أهمية بالغة لما يترتب على بطلان الدليل من آثار، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم، وعليه متى ما شاب التفتيش الواقع عل الحاسوب عيب فإنه يبطله، كما أن التفتيش الذي يقوم به المحقق بغير الشروط التي نص عليها القانون يعتبر باطلا بطلانا مطلقا ولا يجوز التمسك بما ورد في محضر التفتيش، كما لا يجوز للمحكمة أن تعتمد عليه في حكمها[2].

ونؤيد من جانبنا هذا المسلك حيث يتناسب مع طبيعة الدليل الرقمي الذي يؤدي بالضرورة إلى اختلاف قواعده في الاثبات عن غيره من صور الدليل الجنائي في الجرائم الأخرى التي يمكن التوسع في أدلتها، وبالتالي تحري درجة مصداقيتها بحسب نوعها من جهة مع مراعاة ظروف وملابسات القضية من جهة

---

[1] – صفاء حسن نصيف، مرجع سابق، ص 263.

[2] – أنظر: علي حسن الطوالبة، "مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)"، مركز الاعلام الأمني، ص 3، الموقع الالكتروني: (تاريخ الزيارة 2017/12/15) https://www.policemc.gov.bh/.../a79e37dc-9beb-4511-baec-21afff.

أخرى وظروف الحصول عليه، وإن كان الأمر يتطلب تنظيما قانونيا خاصا للدليل الرقمي من حيث كيفية واجراءات استخلاصه، وسلطة القاضي إزاؤه.

المطلب الثاني: صعوبة وتعقيد اجراءات التحقيق في الجريمة المعلوماتية

من الثابت فقها وقضاء أن الجرائم التقليدية تتسم بطابعها المادي والمحدد على إعتبار أنها ترتكب في إقليم معين، وتحدث أثرها في حدود إقليم تلك الدولة[1]،مما يسهل معه مواجهتها ومتابعة مرتكبيها في ضوء الأحكام القانونية الواردة في التشريعات الجنائية الداخلية لتلك الدولة، لكن هذا يقف على طرف نقيض مع التطورات التكنولوجية التي يشهدها عالمنا المعاصر في مجال المعلوماتية والاتصال أين لجأ الكثير من المجرمين إلى ارتكاب جرائم تقليدية بطرق وتقنيات حديثة، وذلك من خلال الاستخدام غير المشروع لشبكة الإنترنيت أو بواسطتها[2].

هذا الأمر يضعنا أمام معادلة غير متكافئة طرفها أجهزة البحث والتحري مع نقص خبرتهم في مجال المعاملات الالكترونية، والطرف الآخر قراصنة محتالون يتمتعون بمهارات عالية ويواكبون كل جديد في مجال الاتصال

---

[1]- نوفل علي عبد الله الصفو، "جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، دراسة مقارنة"، المجلة المصرية للدراسات القانونية والاقتصادية، العدد الثالث، يناير 2015 ، ص 23.

[2]- نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، ص 30.

والمعلوماتية[1].

ومؤدى ذلك أن جرائم المعلومات لم تعد فقط ترتكب على مستوى محلي محدود بل أصبحت في أغلب صورها من الجرائم العابرة للحدود الدولية، إذ غالبا ما ترتكب في إقليم دولة معينة ويكون ضحاياها في دولة أخرى، لذا تعد هذه الخاصية من أبرز التحديات الاجرائية المرتبطة بالمتابعة الجزائية للجرائم المعلوماتية. وفي هذا الصدد من المتصور اليوم أن يتم اختراق كمبيوتر يوجد في بلد آخر أو إتلاف معطياته[2]، دون أن تكون الحدود الجغرافية حائلا أمام ذلك، طالما أنها تتم في فضاء معلوماتي لا يعترف بالحدود[3]، الأمر الذي يشكل تحدياً حقيقيا لمختلف الأنظمة، لاسيما في ظل الصعوبات الكبيرة في تعقب مرتكبي هذه الجرائم، بسبب الإشكالات القانونية التي المترتبة عنها[4]، خاصة ما تعلق منها بصعوبة ضبط هذه الجرائم وإثباتها وكذا صعوبة تحديد جهة الاختصاص والقانون الواجب التطبيق كما رأينا سابقا.

فضلا على أنه من الصعوبة بمكان ملاحقة المشتبه فيهم بسبب تعقد عملية الربط بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية[5]، وامتداد التفتيش إلى نظام غير النظام

---

[1] – بوقرين عبد الحليم، "حتمية انشاء ضبطية خاصة بالجرائم الالكترونية"، مجلة العلوم القانونية والسياسية، جامعة تكريت، العراق، المجلد الخامس، العدد الأول، 2016، ص102.

[2] – سميرة معاشي، مرجع سابق، ص281.

[3] – نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2008، ص 50.[3]

[4] – سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الله، المرجع السابق، ص 49.

5 – see European Crime Prevention Network, Op.Cit., p.12.

محل الاشتباه، الأمر الذي يصطدم بمدى قانونية هذا الإجراء من حيث مساسه بحق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش، وعلاوة على ذلك فإن عملية الضبط القضائي ينصب على أشياء ذات طبيعة معنوية لا مادية، تكون عرضة للتلف أو التبديل أو المحو[1]، الأمر الذي يحول دون إمكانية معرفة مكان تواجد هذا الشخص، وبالتالي صعوبة ملاحقته.

بناء على ما تقدم سوف نتعرض إلى خصوصية الأحكام الناظمة للتحقيق في جرائم المعلومات، مع بيان موقف المشرع الجزائري في هذا الصدد.

1- خصوصية الأحكام الناظمة للتحقيق في جرائم المعلومات:

إن أهم تحدي يواجه جهات التحقيق المختصة تقنيا في تتبع واقتفاء أثر جرائم المعلومات تمهيدا للقبض على الجاني يتمثل أساسا في ضبط حدود مسرح الجريمة وما يرتبط به من عمليات فنية تسهل عملية الوصول إلى الحقيقة، وإذا كان من السهولة تصور ذلك بالنسبة للجرائم المادية، فهو لا ينطبق بالضرورة على جرائم المعلومات أين تتجرد بطبيعتها من تلك العمليات[2].

[1] – طالب جواد عباس، عبد الجبار ضاحي عواد، المرجع السابق، ص 63.

[2] – ذلك أن مسرح الجريمة بمدلوله المادي ينصرف إلى ذلك المحيط والمكان المباشر الذي ارتكب فيه حادث اجرامي معين والذي يتوقع تبعا له أن توجد فيه أغلب الآثار الجنائية، بحيث يمكن عزله بطرق تتناسب مع نوع مسرح الجريمة سواء كان مغلق (منزل، محل تجاري...) أو مفتوح (شارع، غابة...)، ويخضع مسرح الجريمة طبقا لما سبق لجملة من العمليات الفنية التي يتولاها أخصائيين تقنيين وهي تتعلق أساسا بتصوير مسرح الجريمة، ومعاينته، وإعادة تمثيله.

هذا ما يطرح في كل مرة إشكالية قبول الوسائل المتعارف عليها في التحقيق وفي مقدمتها اجراء المعاينة والتفتيش من حيث انطباقها على جرائم المعلومات في صورها المختلفة.

يمكن القول في هذا الصدد أن التحقيقات التي تجريها جهات التحقيق في الجرائم المعلوماتية تتطلب مزيجا من تقنيات عمل الشرطة التقليدية والجديدة، وتبعا لذلك فهي تتضمن البحث العام، والمصادرة، وصولا إلى الاجراءات المتخصصة كحفظ البيانات الحاسوبية، مع تعذر الأخذ في عدة دول بإجراءات متقدمة مثل التحاليل الجنائية الحاسوبية عن بعد، ويبقى من المهم الاشارة أن الاجراءات المتخصصة الأخرى كجمع البيانات والنفاذ إلى محتواها تتطلب معايير أكثر صرامة كوجود دليل على ارتكاب جريمة خطيرة أو دليل على وجود سبب محتمل أو أسس معقولة[1].

كما تتطلب فضلا عن ما سبق وجود جهاز ضبط للتحقيق مستقل عن أجهزة التحقيق الأخرى يضطلع بمهمة البحث والتحري في مجال الجريمة المعلوماتية[2].

---

[1] – فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبيرانية، دراسة شاملة عن مشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، فيينا، فبراير 2013، ص25، .VB80337 (UNODC/CCPJ/EG4/2013/2)

[2] – من بين الدول السباقة في مجال انشاء ضبطية خاصة بمكافحة الجريمة المعلوماتية نجد الولايات المتحدة الأمريكية التي أنشأت مجموعة من الوحدات من بينها المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيات المعلومات والاتصالات، قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية، وكذا معهد أمن الحواسيب ووحدة جرائم الانترنت، كما استحدث في ولاية أوهايو ما يعرف بشرطة الانترنت، والتي يتمثل دورها في حماية المواقع التي تتعاقد=

من جانب آخر يعد التفاعل بين جهات التحقيق ومقدمي خدمات الانترنت والمعلوماتية محركا رئيسا في البحث والتحقيق طالما أن لدى مقدمي تلك الخدمات المعلومات الخاصة بالمشتركين والفواتير وسجلات الاتصال، ومعلومات عن مواقع الاتصال ومحتواها، وتختلف المقتضيات القانونية الوطنية والسياسات المتبعة في القطاع الخاص بشأن الاحتفاظ بالبيانات، وإفشائها اختلافا كبيرا حسب البلد والقطاع المعني، ونوع البيانات، وفي هذه الحالة يتم اللجوء الى أوامر قضائية للحصول على أدلة من مقدمي الخدمات[1].

فضلا على ما سبق ينبغي أن يكون المحقق لديه القدرة على معرفة الصيغ المختلفة للملفات وتطبيقات الحاسوب التي تتعامل معها،إذ تعد الملفات الوعاء الحقيقي لأدلة الادانة في كثير من القضايا المتعلقة بشبكة الانترنت بما تحويه من معلومات،ولا يكفي في المحقق الجنائي في جرائم تقنية المعلومات أن يكون ملما بالقوانين الجنائية التي يتشكل منها التحقيق الجنائي، بل عليه أن يتزيد من المعلومات العامة وسائر العلوم والقوانين المتعلقة بتكنولوجيا المعلومات والاتصالات وشبكة الانترنت، وكلما زادت معلوماته العامة كلما أدى ذلك الى زيادة خبرته ودرايته، ومن تلك القوانين: القانون الالكتروني، قانون المعاملات والعقود الالكترونية، قانون الاثبات باستخدام التوقيع الالكتروني، قانون مكافحة جرائم النظم المعلوماتية، ومن العلوم علم النفس بوجه عام علم النفس

=معها رسميا نظير مقابل مادي، وفي فرنسا قام المشرع الفرنسي بإنشاء المكتب المركزي لمكافحة الاجرام المتعلق بتكنولوجيا المعلومات والاتصال والذي يتواجد على مستوى المديرية المركزية للشرطة القضائية، كما تم انشاء قسم الانترنت الذي يتبع الدرك الوطني./ راجع بخصوص هذا الموضوع: بوقرين عبد الحليم، مرجع سابق، ص ص 156، 157.

[1]- فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبيرانية، مرجع سابق، ص 26

الجنائي بوجه خاص، علم الاجتماع علم الاجرام، ومما تجب الاشارة إليه في هذا السياق أن إلمام المحقق بهذه العلوم لا يقتضي المام المتخصص فيها والعالم ببواطن ودقائق الامور، بل يكفي أن يكون ملما بأساسياتها[1].

الجدير بالإشارة بعد كل ما سبق ذكره أن الحديث عن التحقيق الجنائي المترتب عن جرائم المعلومات بمدلوله الفني لا ينفصل عن إجراء مهم، ألا وهو "التفتيش المعلوماتي".

قبل الخوض في تفاصيل هذا الموضوع من الضروري والمهم الاشارة أن التشريعات الاجرائية المقارنة ومن ضمنها التشريع الجزائري لم تتعرض إلى تعريف التفتيش بوجه عام بقدر اهتمامها بتحديد ضوابطه ومقتضياته، وهذا بالنظر إلى كونه إجراء خطير يترتب عليه حتما المساس بحق الخصوصية.

في المقابل قدم الفقه بعض التعريفات المناسبة لطبيعة وهدف هذا الاجراء، ومنها أنه وسيلة من وسائل البحث في الجرائم للحصول على أدلة إثبات لتسليط العقوبات المنصوص عليها بالقانون الجنائي على الفاعلين الأصليين والشركاء، فهو الاجراء الذي يؤذن به لجمع الأدلة عن جريمة وقعت بالفعل وقامت دلائل وشبهات قوية على اتهام شخص معين، فليس القصد من التفتيش استكشاف الجريمة، بل الغرض منه هو استكشاف أدلتها وآثارها، وكل ما يكون قد استعمل في ارتكابها أو نتج عنها[2].

والتفتيش في مدلوله القانوني بالنسبة لجرائم المعلومات لا يختلف وفقا لما ذهب إليه جانب من الفقه عن مدلوله السائد في فقه الاجراءات الجزائية،

---

[1]– طه السيد أحمد الرشيدي، مرجع سابق، ص 56.

[2]– برهان عزيزي، مرجع سابق، ص 136.

حيث يكون المقصود منه التنقيب في وعاء السر بهدف ضبط ما يفيد في كشف الحقيقة، وعليه يكون هدف التفتيش في جرائم المعلومات الوصول إلى ما تحويه نظم المعلوماتية من أشياء تفيد في كشف الحقيقة ونسبتها إلى المتهم، أو هو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، ويستوي في ذلك المحل أن يكون جهاز الحاسب الآلي أو نظمه أو شبكة الانترنت.

ولا يفوتنا الاشارة في ذات السياق أن التفتيش باعتباره وسيلة للإثبات المادي يتعارض مع الطبيعة غير المادية لبرامج، وبيانات الحاسب الآلي، وكذلك شبكة الانترنت على اعتبار أنها مجرد بيانات ليس لها أثر مادي ملموس في العالم الخارجي[1]. وأمام هذا الوضع نشأ سجال فقهي انصب حول البحث في مدى صلاحية المكونات غير المادية للوسائط المعلوماتية لتكون محلا للتفتيش المعلوماتي.

يذهب رأي فقهي بخصوص هذه المسألة إلى التمسك بعدم شمول المفهوم المادي للتفتيش على البيانات المتضمنة في الأنظمة المعلوماتية، وبالتالي فإن الضبط القضائي لا يتصور إلا اذا اتخذت بيانات الحاسب الالكتروني شكلا ماديا، ومثال ذلك ألمانيا، فالأدلة المضبوطة يجب أن تكون ملموسة، فالبيانات تنقصها بالضرورة الخاصية المادية وبالتالي لا تشكل أشياء يمكن ضبطها، لكن اذا تم طبع هذه البيانات، فإن هذه المطبوعات يمكن ضبطها، ويتم هذا الضبـط بتصوير

---

[1] – أسامة بن غانم العبيدي، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، نوفمبر، ديسمبر 2013، المجلد 29، العدد 58، ص 87.

الشاشة أو نقلها على حافظة بيانات[1].

ويرى أصحاب هذا الرأي أن هذا الموضوع يشكل في النهاية نقصا تشريعيا يستلزم التعديل مما يستدعي ضرورة النص صراحة على أن يشمل التفتيش البيانات المعالجة الكترونيا، بحيث تصبح الغاية الجديدة بعد التطور التقني وثورة الاتصالات لا تقتصر على الأدلة المادية، بل تشمل أيضا البيانات المعالجة عبر الحاسب الآلي[2].

وهذا يعني أنه على الرغم من أن حماية المعلومات تشهد تطورا مستمرا بالمقارنة مع حماية الأموال المادية، إلا أن ذلك يحدث دون الوضع في الاعتبار خصائص الأموال المعنوية، لهذا يجب أن تكون هناك استجابات قانونية حديثة للتحديات الحالية لمجتمع المعلومات، ففي الولايات المتحدة الأمريكية،والمملكة المتحدة مثلا، فإنه وعلى الرغم من أن الأدلة غير ملموسة إلا أنه يمكن ضبط السجلات المعالجة ذاتها أو المستندات الناتجة عنها وضبط الحاسب ذاته باعتباره دليلا[3].

وبعيدا عن الرأي السابق فضل جانب آخر من الفقه عدم البحث في دلالات النصوص والخوض في تفسيراتها، وانطلق من منظور واقعي يتطلب بطبيعة الحال أن تتخذ هذه البيانات شكلا ماديا لكي يتم ضبطها وتقديمها للقضاء، وبالتالي

---

[1] - علاء عبد الباسط خلاف، الحماية الجنائية للحاسب الالكتروني والانترنت في ضوء (قانون العقوبات، قانون الاجراءات الجنائية، قانون حماية الملكية الفكرية، مع الاشارة لتصرفات النيابة العامة وأحكام المحاكم الابتدائية ومحكمة النقض)، معهد الكويت للدراسات القضائية والقانونية، الطبعة الثانية، 2008- 2009، ص 404.

[2] - صفاء حسن نصيف، مرجع سابق، ص 266.

[3] - علاء عبد الباسط خلاف، مرجع سابق، ص 404.

فهو يرى أن التفتيش يقع على مكونات الحاسب الآلي ويشمل أيضا البيانات مضافة الى الدعامات التي يمكن أن تحملها مهما كان شكلها، ويعتبر هذا الموقف أكثر اتساقا والبيئة التي يتم فيها التفتيش، فلا مبرر من الاقتصار على الأدلة المادية في التفتيش طالما أنه يوجد دليل غير مادي يؤدي إلى كشف الحقيقة في جريمة معلوماتية معينة يمكن التوصل إليه باتباع تقنيات فنية مما يسهل استخراجه في شكل مادي يمكن تقديمه أمام القضاء على أن ذلك لا يغني بطبيعة عن معالجة القصور التشريعي لموضوع التفتيش في مجال الجريمة المعلوماتية[1].

ومهما يكن من أمر،وحتى يحقق التفتيش المعلوماتي غرضه والمتمثل في تحصيل الدليل، ينبغي قصر مباشرته على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الآلي والشبكات ونظم المعلومات واسترجاع المعلومات، والذين يجب أن يكونوا قد تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية[2].

2- موقف المشرع الجزائري من التحقيق في جرائم المعلومات:

لم يخص المشرع الجزائري الجريمة المعلوماتية بأحكام اجرائية خاصة ومفردة في قانون الاجراءات الجزائية تتعلق بكيفيات سير اجراءات التحقيق والمتابعة، لكنه في المقابل حدد بعض التدابير التي تهدف الى اقتفاء أثر الجريمة المعلوماتية، واستخلاص الأدلة الرقمية منها بموجب أحكام القانون

[1]– صفاء حسن نصيف، مرجع سابق، ص ص 267، 268.

[2]– طه السيد أحمد الرشيدي، مرجع سابق، ص 82.

رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها[1].

إن البحث في هذه المسألة يقتضي منا التطرق إلى النقاط التالية:

أ- الجهات المختصة بإجراء التفتيش المعلوماتي:

تحكم عملية التفتيش المعلوماتي جملة من الضوابط القانونية تحدد صفة القائمين بهذه المهمة أين تختلف من دولة إلى أخرى حسب التشريعات المعمول بها، فهناك من يعهد بهذا الأمر إلى المدعي العام فقط، وهناك من يخول جهة التحقيق القيام بها، والبعض الآخر يكلف الضبطية القضائية لتولي هذه القضية، ولم يحد المشرع الجزائري عن هذا الاتجاه، فبقراءة أحكام المادة 5 من القانون 04/09 نجد أنه قد كلف كل من السلطات القضائية والمتمثلة في النيابة العامة وجهة التحقيق وكذا ضباط الشرطية القضائية القيام بإجراء عملية التفتيش المعلوماتي كقاعدة عامة[2].

غير أنه قد خص حالة وحيدة والتي توصف على أنها من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة والمنصوص عليها في المادة 4 فقرة أ من القانون السالف الذكر بإجراء منفرد بخصوص عملية التفتيش عن باقي الحالات الموجبة لذلك، أين منح المشرع الجزائري سلطة إجراء التفتيش في مثل هذه الجرائم للنائب العام لدى مجلس قضاء الجزائر والذي يمنح بدوره لضباط

---

[1] - القانون رقم 04/09 المؤرخ في 2009/08/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، بتاريخ 2009/08/16، ص 05.

[2] - رضا هميسي، "تفتيش المنظومة المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، العدد 5، جوان 2012، ص 171.

الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته إذنا لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية والإجراءات المتبعة حيال هذه القضية[1].

لعل السبب الرئيس الذي يقف وراء حصر المشرع للجهات المخول لها القيام بعملية التفتيش المعلوماتي يكمن في مراعاة الدقة في التعامل مع الأجهزة والبرامج الموجودة عليها المعطيات، كما أن صعوبة التحقيق في مثل هذا النوع من الجرائم وتعقد عملية الكشف عن مرتكبي الجرم، دفع إلى اقتصار جهة التفتيش على أهل الاختصاص ما تقتضيه طبيعة السرية ودقة وحنكة في التعامل مع المعطيات الالكترونية الشديدة الحساسية وسريعة التلف من أجل الوصول إلى أدلة الإثبات الكافية لإدانة مرتكبي الفعل[2].

ب- حدود إجراء عملية التفتيش المعلوماتي:

تستهدف عملية التفتيش المعلوماتي القيام بعملية البحث في نطاق منظومة معلوماتية أو جزء منها وكذا المعطيات المخزن فيها، ومنظومة تحزين المعلوماتية[3]، حيث يمكن القيام بذلك في مكان ارتكاب الجريمة أو عن بعد[4].

حيث ينصب التفتيش وفقا للمشرع الجزائري في مثل هذه الجرائم على مستودع السر الذي يحتفظ به الشخص بالأشياء المادية والمعنوية التي تتضمن

---

[1]-يزيد بوحليط، "تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري"، مجلة تواصل في الاقتصاد والإدارة والقانون، جامعة عنابة، العدد 48، ديسمبر 2016، ص 87.

[2]- رضا هميسي، مرجع سابق، ص 172.

[3]- المادة 05 من قانون 04/09، مصدر سابق، ص 06.

[4]- معتوق عبد اللطيف، مرجع سابق، ص 132.

نشاطاته المنجزة، ويشمل كل ماله علاقة بالنظم المعلوماتية من برامج وآلات وكذا أجهزة الحاسوب أو الهواتف النقالة وغيرها من الأجهزة الالكترونية التي استند إليها الفاعل للقيام بجريمته مثل شرائح الهواتف وبطاقات الذاكرة وآلات التصوير الرقمية...الخ، أين يمتد هذا التفتيش ليشمل الأشخاص ومساكنهم التي توجد فيها هذه المعدات أو الأماكن التي يتداولون عليها. فعادة ما تقام مثل هذه الجرائم في مقاهي الانترنت محاولة من طرف الفاعلين لتمويه الأجهزة الأمنية وتصعيب من مهمة اكتشاف الفاعل نظرا للعدد الكبير من رواد مثل هذه الأماكن[1].

كما أنه ونظرا للطابع الإقليمي والدولي الذي قد تأخذه مثل هذا النوع من الجريمة فقد أجاز المشرع الجزائري تمديد الاختصاص السلطات المعنية بإجراء عملية التفتيش للقيام بهذه المهمة على مستوى الوطني وكذا خارج الوطن إن اقتضت الضرورة إلى ذلك.

فبالنسبة للمعطيات المبحوث عنها والمخزنة في منظومة معلوماتية أخرى والتي يمكن الوصول إليها انطلاقا من المنظومة الأولى أجاز المشرع الجزائري في هذه الحالة القيام بعملية التفتيش المعلوماتي بسرعة دون الحاجة لاستصدار إذن قضائي من أجل مباشرة العملية حيث يكفي فقط إعلام السلطة القضائية المختصة بذلك، ولعل السبب الذي يكمن وراء هذا الإجراء هو الخوف من اندثار وتلاشي الدليل الذي يحوزه المجرم في حالة إطالة إجراءات وانتظار الحصول على إذن قضائي لمباشرة عملية تفتيش المنظومة حيث قد يعمد المتهم إلى القيام بعملية إتلاف البيانات أو المعطيات التي بحوزته بمجرد وصول إلى علمه أنه

[1]- رضا هميسي، مرجع سابق، ص ص 166، 167.

محل متابعة قضائية من طرف الجهات القضائية لذا ومن أجل تسريع عملية التفتيش اكتفى المشرع بضرورة إعلام السلطات القضائية الإقليمية المختصة[1].

كما خول المشرع الجزائري للسلطات المختصة بإجراء عملية التفتيش اللجوء أو تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[2].

أما في الحالة التي تكون فيها المعطيات المراد تفتيشها واقعة خارجة نطاق إقليم الوطني والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، فقد سمح المشرع الجزائري بالحصول على المعلومات المتعلقة بها في إطار التعاون الدولي من خلال اللجوء إلى طلب المساعدة من السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[3]، فالتطور التكنولوجي الحاصل في مجال المعلوماتية سهل نوعا من ارتكاب الجرائم العابرة للدول، لذلك أصبح من الضروري البحث في مدى مشروعية القيام بإجراء التفتيش المعلوماتي لأحد المتهمين في نطاق دولة أخرى[4].

إن حصول على مثل هذه المعلومات دون طلب المساعدة القضائية يعد بمثابة انتهاكا لسيادة دولة أخرى وخرقا للقوانين الوطنية والاتفاقيات الدولية

---

[1] – رضا هميسي، مرجع سابق، ص ص 167، 168.

[2] – المادة 5 من القانون 04/09، مصدر سابق، ص 6.

[3] – المادة 5 من نفس المصدر.

[4] – عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة الماجستير في العدالة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، ص 96.

المتعلقة بإمكانية التعاون الدولي في مجال مكافحة الجرائم بشكل عام والجرائم المعلوماتية على وجه الخصوص.

وهو الاتجاه الذي أيده القضاء الألماني في أحدى أحكامه الفاصلة في جريمة الغش المعلوماتي أين أيد القضاء الألماني هذا الاتجاه بخصوص قضية البحث في إحدى جرائم الغش المعلوماتي والتي كان يتواجد فيها حاسب آلي في ألمانيا متصل بشبكة اتصالات متواجدة في سويسرا أين كانت تتم عملية تخزين البيانات الغير المشروعية فيها وعند محاولة السلطات الألمانية المختصة الحصول على تلك المعلومات لم يتسنى لها هذا الأمر إلى باللجوء إلى طلب المساعدة القضائية من طرف الدولة السويسرية للفصل في القضية.

هذا ويمكن حسب المادة 32 من اتفاقية بودابست لسنة 2001 الدخول بغرض التفتيش والضبط في أجهزة الحاسب الآلي أو شبكات تابعة لدولة أخرى دون الحصول على إذنها في حالتين تتعلق الأولى بعملية التفتيش بمعلومات أو بيانات متاحة للعامة، والثانية إذا رضي المالك أو حائز هذه البيانات بهذا التفتيش[1].

لكن رغم الاتفاقيات الدولية الموقعة في هذا الشأن والقاضية بإمكانية التعاون في مجال التفتيش المعلوماتي إلا أن الواقع يكشف أن غالبية الدول غير مستعدة لمباشرة هذه الآلية كونها جلها تعتبر مثل هذه القضايا بمثابة مساس بالأمن الداخلي والقومي لها خاصة إذا كان طابع الجريمة يأخذ وصف جريمة

---

[1] – راجع الملحق الخاص بالنص الكامل باتفاقية بودابست المتعلقة بالجريمة الالكترونية.

ماسة بأمن الدولة. وهو ما يصعب من عملية التفتيش في الجرائم ذات البعد الدولي[1].

ج- حجز المعطيات المعلوماتية:

بعد مباشرة عملية التفتيش من طرف السلطات المختصة واكتشاف معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من ضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال الأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[2].

يلاحظ أن المشرع الجزائري استعمل مصطلح دعامة تخزين الكترونية تكون قابلة للحجز ووضع في أحراز أي أقراص مرنة والصلبة وكذا الأشرطة المغناطيسية...الخ، كما نجد أنه فسح المجال أمام ظهور تقنيات تخزين جديدة في المستقبل بالنظر إلى التطورات التي تعرفها مثل هذه التقنيات، فنظرا لصعوبة التعامل مع هذا النوع من المعطيات والتي هي بمثابة ذبذبات الكترونية أو إشارة ممغنطة إلا بعد نسخها على هذه الدعامات[3].

[1]- أسامة بن غانم العبيدي، مرجع سابق، ص ص 93، 94.

[2]- المادة 06 من القانون 04/09، مصدر سابق، ص 7.

[3]- يزيد بوحليط، مرجع سابق، ص ص 90، 91.

ج-1- الحجز عن طريق منع الوصول إلى المعطيات:

في حالة استحالة إجراء الحجز وفقا لما تم الإشارة إله سابقا لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع وصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

ج-2- حدود استعمال المعطيات المتحصل عليها:

لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات التفتيش المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[1].

ما يمكن التنويه إليه في هذا الجانب أن المشرع الجزائري لم يشر إلى الأسباب التقنية التي تعيق عملية الحجز بنمطها الأول والتي تستدعي اللجوء إلى عملية الحجز عن طريق منع الوصول إلى المعطيات، فهل يتعلق الأمر في هذه الحالة بالمنظومة المعلوماتية نفسها من خلال تواجد كلمة سر أو نظام حماية ذات فعالية أكبر يصعب اختراقه، أو أن المشكل يتمثل في صعوبة في عملية نسخ تلك المعطيات لانعدام التقنيات الالكترونية اللازمة لذلك، نظرا للتطور التكنولوجي الحاصل في مجال المعلوماتية[2].

لعل السبب الرئيسي الذي يكمن وراء عملية حجز المعطيات هو ضمان الوصول إلى الأدلة المادية والمعنوية في أية لحظة تريدها السلطات المختصة

---

[1] – المادتين: 07 و09 من القانون 04/09، مصدر سابق، ص 07.

[2] – يزيد بوحليط، مرجع سابق، ص 91.

بإجراء عملية التحقيق، وكذا ضمان عدم إتلاف تلك المعطيات من طرف المتهم وبالتالي تلاشي جهود التحقيق والبحث في جريمة المعلوماتية المعروضة عليها.

د- إلتزامات مقدمي الخدمات:

يراد بقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها[1]، حيث ترد عليهم بعض الالتزامات الواجب القيام بها من أجل مساعدة سلطات المختصة بالتفتيش للوصول إلى المجرم المعلوماتي، ويقع على عاتق مقدمي الخدمات القيام بالالتزامات التالية:

د -1- مساعدة السلطات:

يتعين على مقدمي الخدمات الالتزام بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من قانون 04/09 تحت تصرف السلطات المختصة.

كما يتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

د-2- حفظ المعطيات المتعلقة بحركة السير:

يتعين على مقدمي الخدمات في هذه الحالة الالتزام بحفظ مايلي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

---

[1]-المادة الأولى فقرة د من القانون 04/09، مصدر سابق، ص 05.

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

هذا وتحدد مدة حفظ المعطيات المذكورة سابقا بسنة واحدة ابتداء من تاريخ التسجيل، وأن أي اخلال بالالتزامات السابقة من شأنه إقامة المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية وإمكانية الخضوع لعقوبة قد تصل إلى الحبس من ستة(6) أشهر إلى غاية خمس (5) سنوات وبغرامة من 50,000 إلى 500,000 دج أما الشخص المعنوي فيخضع لعقوبة الغرامة المقررة وفقا للقانون العقوبات الجزائري[1].

د-3 - الالتزامات الخاصة بمقدمي خدمة "الانترنت":

زيادة على الالتزامات السابقة يتعين على مقدمي خدمات الانترنت ما يلي:

- التدخل الفوري لسحب المعطيات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها ممكنا.

---

[1] - المادتين 10، 11 من القانون 04/09، مصدر سابق، ص 07.

- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها[1].

إن ما سبق ذكره يعتبر في غاية الأهمية، ذلك أن المصلحة العامة تقتضي من مزودي الخدمات في الجرائم المعلوماتية خاصة ما تعلق منها بالجرائم الماسة بأمن الدولة والأنشطة غير القانونية الممارسة ضدها القيام بإبلاغ السلطات المختصة بعناوين هؤلاء الأشخاص وكذا بريدهم الالكتروني والصفحة الشخصية الأمر الذي يتعين معه في البداية أن يسعى مزودي الخدمات إلى الحصول على المعلومات الخاصة بالأشخاص المستخدمين قبل مباشرة عملية الاستفادة من الخدمة، لكن هذا الأمر لا يعني السماح للمزود الخدمة بالتلاعب بالبيانات المتحصل عليها حيث يقع هو آخر عليه التزام يقضي بعدم استخدام تلك البيانات الشخصية التي في حوزته بما يخالف القانون. بمعنى أن التزامات مزودي الخدمة أكبر من رواد أو المستفدين من الخدمة حيث يقع عليهم التزام حماية بيانات مستخدميهم وتخزينها، وضرورة التبليغ عن الأنشطة غير المباشرة التي يقومون بها[2].

---

[1] - المادة 12 من القانون 04/09، مصدر سابق، ص 08.

[2] - خالد حامد مصطفى، "المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي"، رؤى استراتيجية، مركز الامارات للبحوث والدراسات الاستراتيجية، المجلد الأول، العدد 2، مارس 2013، ص 22.

خاتمة

من خلال ما جاء في محتوى هذا المؤلف يمكن إيراد جملة من النتائج مشفوعة في بعض الأحيان بمقترحات وذلك كما يلي:

- إن أهم إشكال يتصل بموضوع الجريمة المعلوماتية هو فكرة الإلمام بجميع الأفعال الأنشطة الممكنة لهذه الجريمة وهذا بالنظر لكون المجال المعلوماتي سريع التطور الأمر الذي صعب حصر وسائله وتقنياته.

- إن الفوارق الجوهرية بين الجريمة التقليدية والجريمة المعلوماتية تستوجب من المشرع العقابي الإلمام بجميع الأوصاف والأفعال المشكلة لفعل الإجرام المعلوماتي والعمل على توسيع مجال فكره الحماية الجزائية ليستوعب جميع الحالات المحتملة التي يمكن أن تأخذ وصف الجريمة المعلوماتية حفاظا على مبدأ الأمن القانوني وتجنب التعديلات المتتالية للقوانين الجنائية لمواكبة التطورات الحاصلة في الجريمة المعلوماتية.

- يعتبر عامل سهولة ارتكاب الجريمة المعلوماتية وبساطة الوسائل المستعملة فيها مما جعلها جريمة سريعة الانتشار والتطور،كما زاد من حدتها الانتشار الواسع للشبكة العنكبوتية والتي قضت على الحدود الزمانية والمكانية، حيث أضحت هذه الوسائل في متناول الجميع وفي أي وقت، هذا عكس الجرائم التقليدية التي تشهد معداتها نوعا من التضييق والحظر في استعمالها حيث أن مجرد حيازتها دون استعمالها قد يشكل جريمة يعاقب عليها القانون عكس الجريمة المعلوماتية.

- إن الإشكالات القانونية التي تقترن بالجرائم المعلوماتية من حيث القانون الواجب التطبيق وكذا احترافية الجهات القضائية المختصة للبت في مثل هذا النوع من الجرائم لم يقف حائلا أمام التصدي لهذه الجريمة وتوقيع العقاب على مرتكبيها وذلك من خلال وضع وتبني آليات قانونية آنية وإبرام الاتفاقيات الدولية في هذا المجال من أجل العمل سويا بين أطياف المجتمع الدولي على مكافحة هذه الجريمة والحد من خطورتها تطبيقا لمبدأ عالمية النص الجنائي.

- أدى قصور وسائل الإثبات الجنائية العادية المتبعة حيال الجرائم التقليدية أدى بالفقه الجنائي إلى توسيع دائرة الوسائل المعتمدة في البحث والتحري إزاء الجرائم المعلوماتية ليشمل الإثبات بالدليل الرقمي، من خلال تحويل المعطيات المعلوماتية والأنظمة الإلكترونية المخزنة على أجهزة الحاسوب كدليل إثبات ضد أصحباها بما يمهد السبيل إلى الوصول للمجرم المعلوماتي.

- إن أهم العوائق الحقيقية التي تقف كحائل أمام مكافحة الجريمة المعلوماتية هو فكرة المساس بالأمن الداخلي والقومي للدول، حيث تعكف غالبية الدول في على عدم فتح مجال التعاون فيما بينها سواء في مجال التحقيق القضائي أو تبادل المعلومات، متمسكة بخطورة مثل هذه الإجراءات على أمنها الداخلي خاصة إذا كانت مثل هذه الجرائم واقعة في أماكن تابعة لأجهزة حكومية أو رئاسة الجمهورية أو المقرات الأمنية.

- رغم الجهود الدولية المبذولة لمكافحة الجريمة المعلوماتية إلى أنها تبقى محدودة وعديمة الفعالية في كثير من الأحيان، الأمر الذي يتطلب مزيدا من تكاثف الجهود والعمل والتشاور وعقد المؤتمرات وإبرام الاتفاقيات الدولية من أجل الوصول إلى أفضل السبل المكنة لمكافحة الجريمة المعلوماتية.

- إن الاتجاه السليم للتقليل من مخاطر الجريمة المعلوماتية إن لم نقل الحد منها نهائيا يقتضي تبني استراتيجية اجتماعية، قانونية وقضائية متكاملة وفق ما يلي:

- إن فعالية مكافحة الجريمة المعلوماتية تنطلق من تبني سياسية وقائية تسبق فكرة السياسية الجنائية الردعية، وذلك نظرا لقصور الأخير ة على الوقوف في وجه الآثار الخطيرة لمثل هذا النوع من الجرائم على الفرد والمؤسسات على حد سواء، وهو ما يحتم طرح حلول إستباقية تراعي تبني وتفعيل برامج وأطر توعوية وتربوية ومنهجية بما يدعم التدخل القانوني بما يكفل تكريس منظومة متكاملة قادرة على مجابهة الجريمة المعلوماتية والحد من خطورتها.

- نظرا لخصوصية الجريمة المعلوماتية وتعقدها وتشعبها يتطلب الأمر تأهيل أفراد تنصيب مؤسسات وهياكل متخصصة في مجال التحقيق القضائي الجرائم المعلوماتية، ذلك أن أجهزة التحقيق التقليدية وبما تتوافر عليه من آليات محدودة الأثر تبقى وحدها عاجزة عن مسايرة هذا النمط الجديد من الجريمة لارتباطها بصفة مباشرة بالأنظمة المعلوماتية لأجهزة الحواسيب وهو ما يجعلها خارج دائرة البحث الفعال والمجدي الذي يضمن الوصول إلى نتائج حاسمة تفضي إلى كشف النقاب عن المجرم المعلوماتي.

- من الضروري والمهم استحداث أقطاب متخصصة على المستوى الدولي في مجال مكافحة الجريمة المعلوماتية، والذي ينطلق من تعزيز أطر التعاون الجماعي بين جميع الدول من أجل ضمان فعالية أكبر ونطاق أوسع للحد من خطورة هذه الجريمة، بعدما أثبت الواقع أن الجهود والمحاولات الفردية والثنائية للدول هنا وهناك قاصرة عن مجابهة المد الخطير للجريمة المعلوماتية الذي تجاوز كل الأمكنة والأزمنة واضعا أمن الدول وسلامة أنظمتها المعلوماتية على المحك.

- العمل على ضبط نشاط فضاءات وأماكن تقديم خدمات الانترنت من خلال إحكام الرقابة المستمرة والدورية على خدماتها من طرف الجهات الادارية المختصة قبليا وبعديا، وذلك بالنظر إلى أنها تعتبر البيئة النشطة والملاذ الأكبر استقطابا للمجرمين المعلوماتيين لارتكاب جرائمهم، فإحكام الرقابة على النحو المتقدم من شأنه تضييق الخناق على فرص الجرم المعلوماتي وإفشال مخططاته، فضلا على أنه يساهم في تسهيل إقتفاء أثره، وجمع ما أمكن من أدلة أو وسائل المستخدمة في ارتكابه للجريمة.

- من الضروري الالتفات والتوجه للاستفادة من احترافية الناشطين والباحثين في مجال الأنظمة المعلوماتية والهاكرز بصرف النظر عن سنهم أو جنسهم أو انتمائهم أو مستواهم التعليمي، بما يسمح بتطوير خبراتهم ومهارتهم وتوظيفها لابتكار البرامج المعلوماتية وأنظمة الحماية والأمن المعلوماتي، وهو ما يتأتى بتوفير فرص الدعم والحوافز لهم.

ملحق يتضمن:

إتفاقية بوادبست لسنة 2001

المتعلقة بالجريمة الالكترونية

مجلس أوروبا
مجموعة المعاهدات
سلسلة المعاهدات الأوروبية – رقم 185
الاتفاقية المتعلقة بالجريمة الإلكترونية
بودابست - 2001/11/23

الديباجة:

إن الدول الأعضاء في مجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية؛ إذ تأخذ في الاعتبار أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛ واعترافاً منها بقيمة تعزيز التعاون مع الدول الأخرى الأطراف في هذه الاتفاقية؛

واقتناعاً منها بالحاجة إلى إتباع سياسة جنائية مشتركة، كمسألة ذات أولوية، بهدف حماية المجتمع من الجريمة الإلكترونية،من خلال تبني تشريع ملائم ودعم التعاون الدولي، من بين أمور أخرى؛

وإدراكاً منها بعمق التغييرات التي أحدثتها الرقمنة والالتقائية والعولمة المتواصلة لشبكات الكومبيوتر؛

وإذ يساورها القلق بشأن مخاطر إمكانية استخدام شبكات الكومبيوتر والمعلومات الإلكترونية أيضا لارتكاب جرائم جنائية، وأنالأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات؛

واعترافاً منها بالحاجة إلى التعاون بين الدول والقطاع الخاص في مجال مكافحة الجريمة الإلكترونية، والحاجة إلى حمايةالمصالح المشروعة عند استخدام وتطوير تكنولوجيا المعلومات؛

وإيماناً منها بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم تعزيز التعاون الدولي في المسائل الجنائية وتسريع وتيرته وتوظيفهبشكل جيد؛

واقتناعا منها بأن هذه الاتفاقية ضرورية لردع الأعمال الموجهة ضد سرية وسلامة وتوافر نظم الكومبيوتر، والشبكات والبياناتبالإضافة إلى إساءة

استخدام هذه النظم والشبكات والبيانات، وذلك بالتنصيص على تجريم سلوكيات من هذا القبيل، كما هو مبين في هذه الاتفاقية واعتماد الصلاحيات الكافية من أجل مكافحة فعالة لمثل هذه الجرائم الجنائية من خلال تيسير كشفها، والتحقيق بشأنها، ومقاضاتها على المستويين الوطني والدولي على حد سواء، وكذلك عن طريق توفير ترتيبات من أجل تحقيق عاون دولي سريع وموثوق؛

وحرصاً منها على ضرورة تأمين التوازن الملائم بين المصالح المتصلة بإنفاذ القانون من جهة واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام ١٩٥٠ بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام ١٩٦٦ المتعلق بالحقوق المدنية والسياسية، وغيرها من المعاهدات الدولية بشأن حقوق الإنسان السارية والتي تؤكد حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير، بما في ذلك حرية البحث عن مختلف أنواع المعلومات والأفكار وتلقيها ونقلها بغض النظر عن الحدود، علاوة على الحقوق المتعلقة باحترام الخصوصية؛

وحرصاً منها كذلك على الحق في حماية البيانات الشخصية، الذي تخوله على سبيل المثال اتفاقية مجلس أوروبا لعام ١٩٨١بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛

وإذ تأخذ في الاعتبار اتفاقية الأمم المتحدة لعام ١٩٨٩ بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام ١٩٩٩ بشأن أسوأ صور عمل الأطفال؛

وإذ تأخذ بعين الاعتبار اتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي، وكذلك المعاهدات المماثلة القائمة بينالدول الأعضاء في مجلس أوروبا وغيرها من الدول، وتؤكد على أن الاتفاقية الحالية ترمي إلى استكمال تلك الاتفاقيات بغية تعزيز فعالية التحقيقات والإجراءات الجنائية

المتعلقة بالجرائم ذات الصلة بنظم وبيانات الكومبيوتر، والتمكين من جمع الأدلة في الجرائم الجنائية ذات الطابع الإلكتروني؛

وإذ ترحب بالتطورات الأخيرة التي تعزز التفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية، بما في ذلك الإجراء الذي اتخذته منظمة الأمم المتحدة، ومنظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي ومجموعة الثمانية

وإذ تذكر بتوصيات لجنة الوزراء رقم ١٠/٨٥ بشأن التطبيق العملي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية، والتوصية رقم ٢/٨٨ بشأن القرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة، والتوصية رقم ١٥/٨٧ التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم ٤/٩٥ بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات مع إشارة خاصة إلى الخدمات الهاتفية، بالإضافة إلى التوصية رقم ٩/٨٩ بشأن الجرائم ذات الصلة بالكمبيوتر التي توفر مبادئ توجيهية للهيئات التشريعية الوطنية بشأن تعريف بعض جرائم الكومبيوتر، والتوصية رقم ١٣/٩٥ بشأن المشاكل التي يطرحها قانون الإجراءات الجنائية علاقة بتكنولوجياالمعلومات؛

ومراعاة للقرار رقم ١ الذي تبناه وزراء العدل الأوروبيون في مؤتمرهم الواحد والعشرين (براغ، في ١٠ و١١ يونيو/حزيران ١٩٩٧) والذي أوصى لجنة الوزراء بدعم الجهود التي تبذلها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) في مجال الجريمة الإلكترونية بغية تقريب أحكام القوانين الجنائية الوطنية من بعضها البعض، وتمكين استخدام الوسائل الفعالة لإجراء التحقيقات في مثل هذه الجرائم، بالإضافة إلى القرار رقم ٣ المعتمد خلال المؤتمر الثاني لوزراء العدل الأوروبيين (لندن، ٨ و٩ يونيو/حزيران ٢٠٠٠) والذي شجع الأطراف المتفاوضة على مواصلة جهودهم بغرض إيجاد حلول

ملائمة لتمكين أكبر عدد ممكن من الدول أن تصبح أطرافاً في الاتفاقية، وأقر بالحاجة إلى نظام سريع وفعال للتعاون الدولي يأخذ بعين الاعتبار وكما يجب الشروط الخاصة بمكافحة الجريمة الإلكترونية؛

وبالنظر لخطة العمل التي اعتمدها رؤساء الدول والحكومات الأعضاء في مجلس أوروبا بمناسبة انعقاد القمة الثانية (ستراسبورغ، ١٠ و١١ أكتوبر/تشرين الأول ١٩٩٧) بغية إيجاد ردود مشتركة لتطور تكنولوجيات المعلومات الحديثة وفقاً لمعايير وقيم مجلس أوروبا؛

اتفقت على ما يلي:

الباب الأول- استخدام المصطلحات

المادة ١- التعريفات

لأغراض هذه الاتفاقية:

أ. يُقصد بـ "منظومة الكومبيوتر" أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات؛

ب. يُقصد بـ "بيانات الكومبيوتر" أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة؛

ج. يُقصد بـــــ " مُقدم الخدمة"

١ (أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و

٢ (أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

د. يُقصد بـ "بيانات حركة الاتصالات" أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءاً

في سلسلة الاتصالات، توضح المنشأ، والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية.

الباب الثاني: التدابير الواجب اتخاذها على الصعيد الوطني

القسم الأول: القانون الجنائي الموضوعي

الفصل الأول: الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكومبيوتر

المادة ٢ – النفاذ غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة ٣ – الاعتراض غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِيّة غير صادقة أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة ٤ – التدخل في البيانات

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً : إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.

٢ .يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة ١ في ضرر جسيم.

المادة ٥ – التدخل في النظام

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها.

المادة ٦ – إساءة استخدام الأجهزة

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق:

أ. عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى:

١ .جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛

٢ .كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛ و

ب. حيازة إحدى المواد المشار إليها في الفقرة أ (١) أو (٢) أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥. ويجوز للدولة الطرف أن تشترط بموجب القانون أن تكون حيازة عدد من هذه المواد سابقة لإلحاق المسؤولية الجنائية.

٢ .لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع، الشراء بغرض الاستخدام، الاستيراد، التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها بالفقرة ١ من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من ٢ إلى ٥ من هذه

الاتفاقية، بل بالأحرى للاستخدام المرخص لغرض اختبار أو حماية نظام الكمبيوتر.

٣ .يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة ١ من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع، توزيع أو إتاحة هذه المواد المشار إليها في الفقرة ١- أ (٢) من هذه المادة.

الفصل الثاني: الجرائم ذات الصلة بالكومبيوتر.

المادة ٧ – التزوير المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: إدخال، تغيير، حذف أو إتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

المادة ٨ – الاحتيال المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ. أي إدخال، تغيير، حذف أو إتلاف لبيانات الكومبيوتر؛

ب. أي تدخل في وظيفة نظام الكومبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق، على منفعة اقتصادية ذاتية أو لفائدة شخص آخر.

الفصل الثالث: الجرائم ذات الصلة بالمحتوى

المادة ٩ – الجرائم ذات الصلة بمواد إباحية عن الأطفال

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق:

أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكومبيوتر؛ ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكومبيوتر؛ ج. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكومبيوتر؛

د. الحصول على مواد إباحية عن الأطفال عبر نظام الكومبيوتر لصالح الشخص ذاته أو لفائدة الغير؛ ه. حيازة مواد إباحية عن الأطفال داخل نظام الكومبيوتر أو على دعامة لتخزين بيانات الكومبيوتر.

٢ .لغرض الفقرة ١ أعلاه، تشمل عبارة "مواد إباحية عن الأطفال" المواد الإباحية التي تعرض بشكل مرئي:

أ.قاصر وهو يمارس سلوكا جنسيا واضحا؛

ب. شخص يبدو قاصرا وهو يمارس سلوكا جنسيا واضحا؛

ج. صور واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا واضحا.

٣ .لغرض الفقرة ٢ أعلاه، يشمل مصطلح " قاصر " كافة الأشخاص دون سن الثامنة عشر. ويجوز لأي دولة طرف أن تشترط حداً عمرياً أدنى لا يقل عن سن السادسة عشر.

٤ .يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين "د" و "ه" من الفقرة ١ والبندين "ب"، "ج" من الفقرة ٢.

الفصل الرابع: الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

المادة ١٠ – الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في ٢٤ يوليو/تموز ١٩٧١ والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق

الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكومبيوتر.

٢ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق ذات الصلة، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة الويبو بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكومبيوتر.

٣ .يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين ١ و٢ من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين ١ و٢ من هذه المادة.

الفصل الخامس: المسؤولية الإضافية والعقوبات

المادة ١١ – المحاولة، والمساعدة والتحريض

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ١٠ من هذه الاتفاقية، وذلك بنِية ارتكاب جريمة من هذا القبيل.

٢ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: محاولة

ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من ٣ إلى ٥، ٧، ٨ و٩. ١ (أ) و(ج) من هذه الاتفاقية.

٣ .يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة ٢ من هذه المادة كلياً أو جزئياً .

المادة ١٢ – مسؤولية الشركات

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن

الجرائم المنصوص عليها في هذه الاتفاقية التي تُرتكب لمصلحتها من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضوا في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قيادياً داخلها، وذلك بناء على:

أ.سلطة تمثيل الشخص الاعتباري؛

ب. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

ج. سلطة ممارسة الرقابة لدى الشخص الاعتباري.

٢ .بالإضافة إلى الحالات المنصوص عليها مسبقا في الفقرة ١ من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان مساءلة الشخص الاعتباري في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة ١ في ارتكاب جريمة منصوص عليها وفقا لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

٣ .رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية، مدنية أو إدارية.

٤ .لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

المادة ١٣ – العقوبات والتدابير

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من ٢ إلى ١١ مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية.

٢ .تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقا للمادة ١٢ وإخضاعهم لعقوبات أو تدابير فعالة، متناسبة ورادعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

القسم الثاني: القانون الإجرائي

الفصل الأول: أحكام مشتركة

المادة ١٤ – نطاق الأحكام الإجرائية

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار السلطات والإجراءات المنصوص عليها

في هذا القسم لأغراض التحقيقات والدعاوى الجنائية المحددة.

٢.باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في المادة ٢١، تطبق كل دولة طرف السلطات والإجراءات المشار إليها في الفقرة ١ من هذه المادة على:

أ. الجرائم الجنائية المقررة في المواد من ٢ إلى ١١ من هذه الاتفاقية؛ ب. الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكومبيوتر؛ و ج. جمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني.

٣.أ. يجوز لكل دولة طرف أن تحتفظ بالحق في تطبيق الإجراءات المشار إليها بالمادة ٢٠ فقط على الجرائم أو أصناف الجرائم المحددة في التحفظ، شريطة ألا يكون نطاق هذه الجرائم أو أصناف الجرائم مقيدا بشكل أكبر من نطاق الجرائم التي تطبق عليها الإجراءات المشار إليها في المادة ٢١. ويتعين على كل دولة طرف النظر في تقييد هذا التحفظ بشكل يمكّن من تطبيق التدبير المشار إليه في المادة ٢٠ على أوسع نطاق.

ب. في حال تعذر على دولة طرف، بسبب قيود موجودة في تشريعاته السارية وقت التصديق على هذه الاتفاقية، تطبيق التدابير المشار إليها في المادتين ٢٠ و٢١ على الاتصالات المنقولة داخل نظام الكومبيوتر لمزود الخدمة، عندما يكون ذلك النظام:

١ .مشغلا لفائدة مجموعة مغلقة من المستخدمين، و

٢ .لا يستخدم شبكات الاتصالات العمومية، وغير متصل بأي نظام كومبيوتر آخر، سواء كان عاما أو خاصا،

فإنه يجوز لتلك الدولة الطرف الاحتفاظ بالحق في عدم تطبيق هذه التدابير على تلك الاتصالات. ويتعين على كل دولة طرف النظر في تقييد هذا التحفظ بشكل يمكِّن من تطبيق التدبير المشار إليه في المادة ٢٠ على أوسع نطاق.

المادة ١٥ – الشروط والضمانات

١ .تسعى كل دولة طرف إلى ضمان خضوع وضع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذا القسم، للضمانات والشروط المنصوص عليها في قانونها الوطني، الذي ينبغي أن يوفر الحماية الملائمة لحقوق الإنسان والحريات، بما في ذلك الحقوق الناشئة عن الالتزامات التي تعهدت بها بموجب اتفاقية مجلس أوروبا لعام ١٩٥٠ الخاصة بحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام ١٩٦٦ الخاص بالحقوق المدنية والسياسية، وغيرها من الصكوك الدولية ذات الصلة بحقوق الإنسان، وأن يدمج مبدأ التناسب.

٢ .تشمل هذه الشروط والضمانات، حسب الاقتضاء بالنظر لطبيعة الإجراءات أو السلطات المعنية، الإشراف القضائي أو بواسطة أي هيئة مستقلة أخرى، والأسس المبررة للتطبيق، وحدود نطاق تلك الإجراءات أو السلطات ومدتها، من بين أمور أخرى.

٣ .بقدر ما يتفق مع المصلحة العامة، خاصة الإدارة السليمة للعدالة، يقوم كل طرف بتدارس تأثير السلطات والإجراءات الواردة في هذا القسم على حقوق الأغيار ومسؤولياتهم ومصالحهم المشروعة.

الفصل الثاني: التعجيل في حفظ بيانات الكومبيوتر المخزنة

المادة ١٦- التعجيل في حفظ بيانات الكومبيوتر المخزنة

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من الأمر أو الحصول على الحفظ المعجل لبيانات كومبيوتر محددة، بما في ذلك بيانات الحركة المُخزنة بواسطة نظام الكومبيوتر، خاصة في حال وجود أسس للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل.

٢ .في حال تفعيل دولة طرف للفقرة ١ أعلاه عبر توجيه أمر إلى شخص من أجل حفظ بيانات كومبيوتر محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكومبيوتر المعنية والإبقاء على سلامتها لأطول مدة زمنية ضرورية على ألا تتجاوز تسعين يوماً ، من أجل تمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف التنصيص على تجديد هذا الأمر لاحقا.

٣ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام القيِّم على حفظ بيانات الكومبيوتر أو أي شخص آخر عهدت له هذه المهمة، بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانونها الوطني.

٤ .تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

المادة ١٧ — التعجيل في حفظ بيانات الكومبيوتر والكشف الجزئي عن بيانات الحركة

١ .تعتمد كل دولة طرف، فيما يتعلق ببيانات الحركة الواجب حفظها بموجب المادة ١٦، ما يلزم من تدابير تشريعية وغيرها من التدابير بغية:

أ. ضمان توفر إمكانية التعجيل في حفظ بيانات الحركة بصرف النظر عن مشاركة مزود خدمة واحد أو أكثر في عملية نقل هذا الاتصال؛ و

ب. ضمان تعجيل الكشف للسلطة المختصة لدى الدولة الطرف، أو الشخص الذي تعينه تلك السلطة، عن القدر الكافي من بيانات الحركة من أجل تمكين الدولة الطرف من تحديد مزود الخدمة والمسار الذي تم من خلاله نقل الاتصال.

٢ .تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

الفصل الثالث: الأمر بإبراز البيانات

المادة ١٨ – الأمر بإبراز البيانات

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى: أ. أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر.

ب. أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.

٢ .تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

٣ .لغرض هذه المادة، يقصد بعبارة "معلومات عن المشترك" أي معلومات مدرجة في شكل بيانات الكومبيوتر أو في أي شكل آخر يحفظها مزود الخدمة والتي تتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

أ.نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة؛

ب.هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج، والبياناتالخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة؛

ج.أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال والمتاحة بموجب اتفاق أو ترتيبات الخدمة.

الفصل الرابع: البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

المادة ١٩ – البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من البحث عن أو النفاذ إلى:

أ. أي نظام كومبيوتر أو أي جزء منه وبيانات الكمبيوتر المخزنة فيه؛ و

ب. أي دعامة تخزين بيانات الكمبيوتر يمكن أن تكون بيانات كمبيوتر مخزنة داخلها على أراضي تلك الدولة الطرف.

٢ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان أنه في حال إنجاز سلطاتها لعلميات البحث أو النفاذ إلى نظام كومبيوتر أو إلى جزء منه، وفقاً للفقرة ١ (أ) وتوفر أسس لديها للاعتقاد بأن البيانات المطلوبة مخزنة داخل نظام كومبيوتر آخر أو على جزء منه على أراضي الدولة الطرف، وأنه يمكن النفاذ إلى تلك البيانات أو أنها متاحة قانونياً على النظام الأصلي، ينبغي أن تتمكن السلطات من تعجيل توسيع نطاق البحث أو النفاذ إلى النظام الآخر.

٣ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من مصادرة أو تأمين بيانات الكومبيوتر التي تم النفاذ إليها طبقاً للفقرتين ١ أو ٢. وتشمل هذه الإجراءات سلطة:

أ. مصادرة أو تأمين نظام الكومبيوتر أو جزء منه أو دعامة تخزين بيانات الكمبيوتر؛ ب. إجراء نسخة من هذه البيانات الحاسوبية والاحتفاظ بها؛ ج. الحفاظ على سلامة بيانات الكومبيوتر المخزنة ذات الصلة؛

د. جعل تلك البيانات الحاسوبية غير قابلة للنفاذ على نظام الكومبيوتر الذي تم الولوج إليه أو إزالتها.

٤ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من أمر أي شخص لديه معرفة بتشغيل نظام الكومبيوتر أو التدابير المطبقة لحماية البيانات الحاسوبية الموجودة عليه، بتقديم، في حدود المعقول، المعلومات اللازمة لتمكين إجراء التدابير المشار إليها في الفقرتين ١ و٢.

٥.تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

الفصل الخامس: جمع بيانات الكومبيوتر في الوقت الحقيقي

المادة ٢٠- جمع بيانات الكومبيوتر في الوقت الحقيقي

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية، على أراضيها؛ و

ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة على:

١ .جمع أو تسجيل من خلال تطبيق وسائل فنية، عل ؛ أو أراضي الدولة الطرف؛ أو ٢. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات الحركة، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

٢ .في حال تعذر على الدولة الطرف، بسبب المبادئ القائمة في نظامها القانوني الوطني تبني التدابير المشار إليها في الفقرة ١(أ)،يجوز لها بدلاً من ذلك اعتماد تدابير تشريعية وغيرها من التدابير الضرورية لضمان الجمع أو

التسجيل في الوقت الحقيقي لبيانات الحركة المرتبطة باتصالات محددة تم نقلها على أراضيها، من خلال تطبيق وسائل فنية على تلك الأراضي.

٣ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالحفاظ على سرية تنفيذ أي من السلطات المنصوص عليها في هذه المادة وعلى أي معلومات مرتبطة بها.

٤ .تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

المادة ٢١ – اعتراض بيانات المحتوى

١ -تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير، فيما يتعلق بنطاق الجرائم الجسيمة التي يحددها القانون الوطني، لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها؛ و ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة، على:

١ .جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها؛ أو ٢. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات المحتوى، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

٢ .في حال تعذر على الدولة الطرف تبني الإجراءات المشار إليها في الفقرة ١ (أ)، بسبب المبادئ القائمة في نظامها القانوني الوطني، يجوز لها بدلاً من ذلك أن تعتمد ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصالات معينة تم نقلها في أقاليمها عبر تطبيق وسائل فنية في تلك الأقاليم.

٣ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالمحافظة على سرية تنفيذ أي من السلطات المنصوص عليها هذه المادة وأي معلومات متصلة بها.

٤ .تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين ١٤ و١٥.

الباب الثالث: الولاية القضائية

المادة ٢٢ – الولاية القضائية

١ .تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على أي جريمة تنص عليها المواد من ٢ إلى ١١ من هذه الاتفاقية، عندما تُرتكب الجريمة:

أ. داخل أقاليمها؛ أو

ب.على متن سفينة ترفع علم تلك الدولة الطرف؛ أو

ج.على متن طائرة مسجلة بموجب قوانين تلك الدولة الطرف؛ أو

د.من قبل أحد مواطنيها، إذا كانت الجريمة مُعاقبا عليها بموجب القانون الجنائي في مكان ارتكابها أو في حال ارتكاب الجريمة خارج الولاية القضائية الإقليمية لأي دولة.

٢ .يجوز لكل دولة طرف الاحتفاظ بالحق في عدم التطبيق أو التطبيق فقط في حالات أو ظروف معينة قواعد الولاية القضائية المنصوص عليها في الفقرات من ١ (ب) إلى ١ (د) من هذه المادة أو أي جزء منها. ٣. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على الجرائم المشار إليها في الفقرة ١ من المادة ٢٤ من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم متواجدا داخل أقاليمها ولا تقوم بتسليمه إلى دولة طرف أخرى على أساس جنسيته فقط، وذلك بعد التوصل بطلب التسليم.

٤ .لا تستبعد هذه الاتفاقية ممارسة أي دولة طرف لولاية جنائية يقرها قانونها الوطني.

٥ .في حال مطالبة أكثر من دولة طرف بالولاية القضائية على جريمة تقرها هذه الاتفاقية، تقوم الدول الأطراف المهنية، عند الاقتضاء، بالتشاور بغرض تحديد الولاية القضائية الأنسب للمقاضاة.

الباب الثالث: التعاون الدولي

القسم الأول: المبادئ العامة

الفصل الأول: المبادئ العامة ذات الصلة بالتعاون الدولي

المادة ٢٣ – المبادئ العامة ذات الصلة بالتعاون الدولي

تتعاون الدول الأطراف فيما بينها، وفقاً لأحكام هذا الباب ومن خلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولي في المسائل الجنائية وبالترتيبات المتفق عليها بمقتضى التشريعات الموحدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية، على أوسع نطاق ممكن لأغراض إجراءات التحقيقات أو المتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر، أو من أجل جمع أدلة بشأن جريمة جنائية في شكل إلكتروني.

الفصل الثاني: المبادئ ذات الصلة بتسليم المجرمين

المادة ٢٤ – تسليم المجرمين

١ .أ) تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد من ٢ إلى ١١ من هذه الاتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد.

ب) في حال كانت هناك تقرير تطبيق عقوبة دنيا مختلفة بموجب ترتيبات متفق عليها على أساس تشريع موحد أو ذي

الصلة بالمعاملة بالمثل أو بموجب معاهدة تسليم المجرمين، بما في ذلك الاتفاقية الأوروبية بشأن تسليم المجرمين

(سلسة المعاهدات الأوربية رقم ٢٤)، واجبة التطبيق بين طرفين أو أكثر، تُطبق العقوبة الدنيا المنصوص عليها بموجبتلك الترتيبات أو المعاهدة.

٢ .تعتبر الجرائم الجنائية الواردة في الفقرة ١ من هذه المادة مدرجة كجرائم يجب فيها التسليم في أي معاهدة بشأن تسليم المجرمين قائمة بين الأطراف، وتتعهد الدول الأطراف بتضمين هذه الجرائم على أنها جرائم يجب فيها تسليم المجرمين في أي معاهدة بشأن تسليم المجرمين يتم إبرامها فيما بينهم.

٣ .في حالة تلقت دولة طرف تخضع تسليم المجرمين لشرط وجود معاهدة ذات الصلة طلباً بالتسليم من طرف دولة طرف أخرى لا تربطها بها معاهدة لتسليم المجرمين، يجوز لتلك الدولة الطرف اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم فيما يتعلق بأي من الجرائم الجنائية المشار إليها في الفقرة ١ من هذه المادة.

٤ .تعترف الدول الأطراف التي لا تشترط وجود معاهدة لتسليم المجرمين بالجرائم الجنائية المشار إليها في الفقرة ١ من هذه المادة على أنها جرائم يجب فيها تسليم المجرمين فيما بينها.

٥ .يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم أو معاهدات تسليم المجرمين واجبة التطبيق، بما في ذلك الأسباب التي تستند إليها الدولة الطرف المطالبة بالتسليم لرفض التسليم.

٦ .في حال رفض التسليم بشأن إحدى الجرائم المشار إليها في الفقرة ١ من هذه المادة، على أساس جنسية الشخص المطلوب فقط أو لأن الدولة الطرف المطلوب منها التسليم تعتبر أنها ذات الولاية القضائية على تلك الجريمة، تقوم الدولة الطرف المطلوب منها التسليم، بناء على طلب الدولة الطرف مقدمة الطلب، بإحالة القضية على سلطاتها المختصة بغرض المقاضاة ثم بإبلاغ الطرف الطالب بالنتيجة النهائية في الوقت المناسب. وتتخذ تلك

السلطات قرارها وتُجري التحقيقات والمتابعات بنفس الطريقة المطبقة على أي جريمة أخرى ذات طابع مشابه بموجب القانون تلك الدولة الطرف.

٧ .أ) تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر الاعتقال الاحترازي في حال عدم وجود معاهدة تسليم المجرمين.

ب) يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات التي يعينها الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

الفصل الثالث: المبادئ العامة ذات الصلة بالمساعدة المتبادلة

المادة ٢٥- المبادئ العامة ذات الصلة بالمساعدة المتبادلة

١ .توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو بجمع أدلة جريمة جنائية في شكل إلكتروني.

٢ .تعتمد أيضا كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتنفيذ الالتزامات الواردة في المواد من ٢٧ إلى ٣٥. ٣. يجوز لكل دولة طرف، في الظروف العاجلة، المطالبة بالمساعدة المتبادلة أو بوثائق عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، بقدر ما توفره تلك الوسائل من مستويات ملائمة للأمن والتحقق من صحة البيانات (بما في ذلك استخدام التشفير عند الضرورة) مع التأكيد الرسمي بتطبيق تلك الوسائل عندما تطالب بذلك الدولة الطرف المطلوب منه تقديم المساعدة. وتقبل الدولة الطرف المطلوب منها تقديم المساعدة وتستجيب للطلب بأي من وسائل الاتصال العاجلة.

٤ .باستثناء ما تنص عليه تحديدا خلاف ذلك مواد هذا الباب، تخضع المساعدة المتبادلة للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها المساعدة، أو معاهدات المساعدة المتبادلة الجاري بها العمل بما في ذلك الأسس التي ترتكز إليها الدولة الطرف المطلوب منها المساعدة لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها المساعدة ممارسة الحق في رفض المساعدة المتبادلة فيما يتعلق بالجرائم المشار إليها في المواد من ٢ إلى ١١ فقط على أساس أن الطلب يتعلق بجريمة تعتبرها جريمة مالية.

٥ .متى كان مسموحاً للدولة الطرف المطلوب منها المساعدة، طبقاً لأحكام هذا الباب، بتقديم المساعدة المتبادلة في حال وجود جريمة مزدوجة، يُعتبر هذا الشرط مستوفياً بغض النظر عما إذا كانت قوانينها تدرج الجريمة داخل التصنيف ذاته أو تطلق على الجريمة نفس المصطلح للطرف مقدم الطلب، طالما أن السلوك الذي يحدد الجريمة المطلوب تقديم المساعدة بشأنها يشكل جريمة جنائية بموجب قوانينها.

المادة ٢٦ – المعلومات التلقائية

١ .يجوز لدولة طرف، في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجزها في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررة طبقا لهذه الاتفاقية أو أن ذلك قد يؤدى إلى تقديم طلب للتعاون من جانب تلك الدولة الطرف بموجب هذا الباب.

٢ .يجوز للطرف الذي يقدم هذه المعلومات، قبل تقديمها، أن يطلب الحفاظ على سرية تلك المعلومات أو استخدامها فقط وفقاً لشروط مُعينة. وإذا لم يكن بإمكان الدولة الطرف المتلقية لهذه المعلومات الامتثال لهذا الطلب، وجب عليها إشعار الطرف المقدم للمعلومات بذلك، والذي يقرر عندئذ إذا ما كان

يتعين عليه مع ذلك تقديم تلك المعلومات. في حال قبول الدولة الطرف المتلقية بالمعلومات الخاضعة للشروط، وجب عليها الالتزام بها.

الفصل الرابع: الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

المادة ٢٧ – الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

١ .في حالة عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد ومتعلق بمبدأ المعاملة بالمثل بين الدولة الطرف المقدمة للطلب والدولة الطرف المطلوب منها، تطبق أحكام الفقرات من ٢ إلى ٩ من هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة أو ترتيب أو تشريع من هذا القبيل، ما لم توافق الأطراف المعنية على تطبيق أي أو كل البنود الباقية من هذه المادة بدلا منها.

٢ .أ) تقوم كل دولة طرف بتعيين سلطة أو سلطات مركزية مسؤولة عن إرسال طلبات المساعدة المتبادلة والرد عليها، أو تنفيذها أو إحالتها على الجهات المختصة من أجل تنفيذها؛

ب) تتواصل السلطات المركزية مع بعضها البعض بشكل مباشر؛

ج) تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا بأسماء وعناوين السلطات المعينة طبقاً لهذه الفقرة؛

د) يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات المركزية التي تعينها الدول الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

٣ .يتم تنفيذ الطلبات الخاصة بالمساعدة المتبادلة بموجب هذه المادة وفقاً للإجراءات التي يحددها الطرف مقدم الطلب، فيما عدا ما يتعارض مع القانون الدولة الطرف المطلوب منها المساعدة.

٤ .يجوز للدولة الطرف المطلوب منها المساعدة، علاوة على أسس الرفض الواردة في الفقرة ٤ من المادة ٢٥، أن ترفض تقديم المساعدة في حال:

أ. كان الطلب يتعلق بجريمة تعتبرها الدولة الطرف المطلوب منها المساعدة جريمة سياسية أو جريمة لها علاقة بجريمة سياسية، أو

ب. ارتأت تلك الدولة أن تنفيذ الطلب من المحتمل أن يمس بسيادتها، أمنها، نظامه العام، أو بمصالح أساسية أخرى.

٥ .يجوز للدولة الطرف المطلوب منها تقديم المساعدة تأجيل البث في الطلب إذا كان من شأن ذلك إلحاق الضرر بتحقيقات أو متابعات جنائية تنجزها سلطاتها.

٦ .قبل رفض أو تأجيل تقديم المساعدة، تقوم الدولة الطرف المطلوب منها تقديم المساعدة، عند الاقتضاء وبعد التشاور مع الدولة الطرف مقدمة الطلب، بالنظر في إمكانية تنفيذ الطلب جزئياً أو إخضاعه للشروط التي تراها ضرورية.

٧ .تخبر الدولة الطرف المطلوب منها تقديم المساعدة على الفور الدولة الطرف مقدمة الطلب بنتيجة تنفيذ الطلب الخاص بالمساعدة. ويتوجب شرح الأسباب أي رفض أو تأجيل للطلب. علاوة على ذلك، تخبر الدولة الطرف المطلوب منها المساعدة الطرف مقدم الطلب بالأسباب التي تجعل تنفيذ الطلب مستحيلا أو التي من المحتمل أن تؤخره بشكل هام.

٨ .يجوز للدولة الطرف مقدمة الطلب أن تطلب من الطرف المطلوب منه المساعدة الحفاظ على سرية أي طلب يتم تقديمه بموجب هذا الباب علاوة على موضوع الطلب، إلا في حدود ما هو ضروري لتنفيذه. وفي حالة تعذر على الدولة الطرف المطلوب منها المساعدة الامتثال للطلب الخاص بالسرية، وجب عليها فورا إخبار الطرف مقدم الطلب الذي يقرر عندئذ ما إذا كان يتعين مع ذلك تنفيذ الطلب.

٩ .أ) في الحالات الطارئة، يجوز للسلطات القضائية بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات الخاصة بالمساعدة المتبادلة أو المراسلات المتعلقة بذلك إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة. وفي مثل هذه الحالات، يتم إرسال نسخة في الوقت نفسه إلى السلطة المركزية في الدولة الطرف المطلوب منها المساعدة عن طريق نظيرتها في الدولة الطرف مقدمة الطلب.

ب) يجوز تقديم أي طلب أو مراسلة بموجب هذه الفقرة من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول).

ج) في حال تقديم طلب وفقاً للفقرة الفرعية (أ) من هذه المادة وعدم اختصاص السلطة للتعامل مع الطلب، وجب على تلك السلطة إحالة الطلب على السلطة الوطنية المختصة وإخبار الدولة الطرف مقدمة الطلب فور إنجاز الإحالة.

د) يجوز للسلطات المختصة بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات أو المراسلات بموجب هذه الفقرة والتي لا تتضمن أي إجراء إلزامي إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

ه) يجوز لكل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق أو القبول، الموافقة أو الانضمام، إخبار الأمين العام لمجلس أوروبا أن الطلبات المقدمة بموجب هذه الفقرة يجب أن ترسل، من أجل الفعالية، إلى سلطتها المركزية.

المادة ٢٨ – السرية والقيود على الاستخدام

١ .في حال عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد أو المعاملة بالمثل بين الدولة الطرف مقدمة الطلب والدولة الطرف المطلوب منها المساعدة، تطبق أحكام هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة، ترتيب أو تشريع من هذا القبيل، ما

لم تتفق الأطراف المعنية على تطبيق أي من البنود المتبقية من هذه المادة أو كلها بدلا منها.

٢ .يجوز للدولة الطرف المطلوب منها المساعدة تقييد توفير المعلومات أو المواد في إطار تلبية الطلب المقدم بشرط:

أ.الحفاظ على سريتها في حال تعذر إمكانية الاستجابة لطلب المساعدة القانونية المتبادلة في غياب شرط من هذا القبيل، أو

ب. عدم استخدامها في تحقيقات أو إجراءات غير تلك المشار إليها في الطلب.

٣.في حال تعذر على الدولة الطرف مقدمة الطلب الامتثال لأحد الشرطين المشار إليهما في الفقرة ٢، وجب عليها فورا إخبار الطرف الآخر، الذي يقرر عندئذ إذا كان يتعين، مع ذلك، تقديم المعلومات. وفي حال قبول الدولة الطرف مقدمة الطلب لهذا الشرط، وجب عليها الالتزام به.

٤.يجوز لأي دولة طرف تقدم معلومات أو مواد وفقاً لأحد الشروط المشار إليها في الفقرة ٢ أن تطلب من الطرف الآخر توضيح استخدام تلك المعلومات أو المواد علاقة بذلك الشرط.

القسم الثاني: أحكام خاصة

الفصل الأول: المساعدة المتبادلة بشأن التدابير المؤقتة

المادة ٢٩ – التعجيل في حفظ بيانات الكومبيوتر المخزنة

١ .يجوز لأي دولة طرف أن تطالب دولة طرفا أخرى أن تأمر أو تحصل بطريقة أخرى على التعجيل في حفظ بيانات مُخزنة بواسطة نظام كومبيوتر، يوجد على أراضي الدولة الطرف الأخرى، والتي تنوي أن تقدم بشأنها طلبا بالمساعدة المتبادلة من أجل البحث عن بيانات، النفاذ إليها، مصادرتها، تأمينها أو كشفها.

٢.يجب أن يحدد طلب الحفظ الذي يتم تقديمه بموجب الفقرة ١ ما يلي:

أ.الجهة التي تطلب الحفظ؛

ب. الجريمة موضوع التحقيقات أو الإجراءات الجنائية وملخص موجز عن الوقائع المتعلقة بها؛ ج. بيانات الكومبيوتر المخزنة المطلوب حفظها وعلاقتها بالجريمة؛

د.أي معلومات متاحة تكشف عن القيِّم على بيانات الكومبيوتر المخزنة أو عن مكان وجود نظام الكومبيوتر؛

ه.الضرورة الموجبة للحفظ؛ و

و.أن تلك الدولة تنوي تقديم طلب المساعدة المتبادلة من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها،مصادرتها، تأمينها أو الكشف عنها.

٣ .عند استلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه المساعدة باتخاذ كافة الإجراءات الملائمة وذلك لتعجيل حفظ البيانات المحددة وفقاً للقانون الوطني. ولأغراض الاستجابة للطلب، لا يجوز تقييد توفير هذا الحفظ بشرط ازدواجية التجريم.

٤ .يجوز لأي دولة طرف تقيد الاستجابة لطلب المساعدة المتبادلة بشرط ازدواجية التجريم من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها، بالنسبة لجرائم غير تلك المنصوص عليها وفقاً للمواد من ٢ إلى ١١ من هذه الاتفاقية، أن تحتفظ بالحق في رفض طلب الحفظ بموجب هذه المادة في الحالات التي يتوافر لديها فيها أسباب للاعتقاد بأنه يتعذر، في وقت الكشف أو الإفصاح عن هذه المعلومات، استيفاء الشرط الخاص بازدواجية التجريم.

٥.بالإضافة إلى ذلك، يجوز رفض طلب الحفظ فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو جريمة مرتبطة بجريمة سياسية، أو

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

٦ .في حال اعتقاد الدولة الطرف المطلوب منها المساعدة أن الحفظ لن يضمن توافر البيانات مستقبلاً أو أنه سيهدد السرية أو يلحق الضرر بالتحقيقات التي تنجزها الدولة الطرف مقدمة الطلب، وجب عليها فوراً إخبار الدولة الطرف مقدمة الطلب التي يحدد عندئذ إذا ما كان ينبغي، مع ذلك، تنفيذ الطلب .

٧ .يكون أي حفظ يتم تفعيله استجابة للطلب المشار إليه في الفقرة ١ لفترة لا تقل عن ستين يوماً بغية تمكين الدولة الطرف مقدمة الطلب من تقديم طلب للبحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها. بعد تلقي طلب من هذا القبيل، يجب مواصلة حفظ البيانات في انتظار صدور قرار بشأن ذلك الطلب.

المادة ٣٠ – تعجيل الكشف عن بيانات الحركة المحفوظة

١ .في حال اكتشفت الدولة الطرف المطلوب منها المساعدة، أثناء تنفيذ طلب مقدم وفقاً للمادة ٢٩ بحفظ بيانات الحركة المتعلقة باتصال محدد، أن أحد مزودي الخدمة في دولة أخرى مشترك في نقل الاتصال، تقوم الدولة الطرف المطلوب منها المساعدة على الفور بالكشف عن القدر الكافي من بيانات الحركة لتحديد هوية مزود الخدمة والمسار الذي تم من خلاله ذلك الاتصال.

٢ .يجوز حجب بيانات الحركة بموجب الفقرة ١ فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو أنها متصلة بجريمة سياسية، أو

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

الفصل الثاني: المساعدة المتبادلة ذات الصلة بسلطات التحقيقات

المادة ٣١ – المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة

١ .يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها عندما تكون تلك البيانات مخزنة بواسطة نظام كومبيوتر يوجد داخل أراضي الدولة الطرف المطلوب منها المساعدة، بما في ذلك البيانات التي تم حفظها وفقاً للمادة ٢٩.

٢ .تستجيب الدولة الطرف المطلوب منها المساعدة للطلب من خلال تطبيق الصكوك والترتيبات والقوانين الدولية المشار إليها في المادة ٢٣، وطبقاً للأحكام الأخرى ذات الصلة الواردة في هذا الباب.

٣.تتم الاستجابة للطلب بشكل معجل عندما:

أ. توجد أسباب للاعتقاد بأن البيانات ذات الصلة مُعَرضة بصفة خاصة للضياع أو التعديل؛ أو ب. تكون الصكوك والترتيبات والقوانين المشار إليها في الفقرة ٢ تنص على التعجيل في التعاون.

المادة ٣٢ – النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم يجوز لدولة طرف، دون ترخيص من دولة طرف أخرى:

أ.النفاذ إلى بيانات كومبيوتر مُخزنة متاحة للعموم (مصدر مفتوح) بغض النظر عن مكان تواجد البيانات جغرافياً ؛ أو

ب. النفاذ إلى بيانات كومبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كومبيوتر داخل أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور.

المادة ٣٣ – المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي

١ .تقدم الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات الحركة في الوقت الحقيقي المرتبطة باتصالات محددة في أقاليمها والتي يتم

نقلها بواسطة نظام كومبيوتر. وطبقاً لأحكام الفقرة ٢، تخضع هذه المساعدة للشروط والإجراءات المنصوص عليها بموجب القانون الوطني.

٢ .توفر كل دولة طرف مساعدة من هذا القبيل على الأقل فيما يتعلق بالجرائم الجنائية التي يكون فيها جمع بيانات الحركة في الوقت الحقيقي متاحاً في قضية محلية مماثلة.

المادة ٣٤ – المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى

توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات المحتوى في الوقت الحقيقي أو تسجيلها فيما يتعلق باتصالات محددة يتم نقلها بواسطة نظام كومبيوتر بقدر ما تسمح به المعاهدات والقوانين الوطنية واجبة التطبيق.

الفصل الثالث: شبكة على مدار الساعة و7 أيام في الأسبوع

المادة ٣٥ – شبكة على مدار الساعة و٧ أيام في الأسبوع

١ .تعين كل دولة طرف نقطة اتصال متاحة على مدار الساعة وسبعة أيام في الأسبوع بغية ضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني. وتشمل هذه المساعدة تسهيل، أو إذا كان قانونها الوطني وممارستها يسمح بذلك، تنفيذ التدابير التالية بشكل مباشر:

أ.توفير المشورة الفنية؛

ب.حفظ البيانات طبقاً للمادتين ٢٩ و٣٠؛

ج.جمع الأدلة وتوفير المعلومات القانونية وتحديد موقع المشتبه بهم.

٢) .أ) يجب أن تتوفر نقطة الاتصال للدولة الطرف على القدرة على إجراء اتصالات مع مثيلتها في دولة طرف أخرى على وجه السرعة.

.ب) إذا كانت نقطة الاتصال التي تعينها دولة طرف ليست جزءاً من السلطة أو السلطات المسؤولة عن المساعدة المتبادلة الدولية أو عن تسليم

المجرمين، وجب على نقطة الاتصال أن تضمن أنها قادرة على التنسيق مع تلك السلطة أو السلطات على وجه السرعة.

٣ .تضمن كل دولة طرف توفير طاقم حاصل على التدريب والمعدات الضروريين من أجل تسهيل تشغيل الشبكة.

الباب الرابع: الأحكام الختامية

المادة ٣٦ – التوقيع ودخول حيز النفاذ

١ .تفتتح هذه الاتفاقية للتوقيع من قبل الدول الأعضاء بمجلس أوروبا والدول غير الأعضاء التي شاركت في صياغتها.

٢ .تخضع هذه الاتفاقية للتصديق، القبول أو الموافقة. وتودع وثائق التصديق، القبول أو الموافقة لدى الأمين العام لمجلس أوروبا.

٣ .تدخل هذه الاتفاقية حيز التنفيذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ تعبير خمس دول، من بينها ثلاث دول على الأقل من أعضاء مجلس أوروبا، عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين ١ و٢.

٤ .تدخل هذه الاتفاقية حيز التنفيذ، بالنسبة لأي دولة توقع عليها وتعرب بعدها عن موافقتها على الالتزام بها، في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ التعبير عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين ١ و٢.

المادة ٣٧ – الانضمام إلى الاتفاقية

١ .بعد دخول الاتفاقية حيز التنفيذ، يجوز للجنة وزراء مجلس أوروبا، بعد التشاور مع الدول المتعاقدة في الاتفاقية والحصول على موافقتها بالإجماع، توجيه الدعوة لأي دولة غير عضو في المجلس ولم تشارك في صياغة الاتفاقية للانضمام إلى هذه الاتفاقية. ويتم اتخاذ القرار بالأغلبية المنصوص عليها في المادة ٢٠- د من النظام الأساسي لمجلس أوروبا وعن

طريق تصويت الدول المتعاقدة في الاتفاقية بالإجماع المخول لها المشاركة في لجنة الوزراء.

٢ .تدخل الاتفاقية حيز التنفيذ – بالنسبة لأي دولة تنضم للاتفاقية بموجب الفقرة ١ أعلاه – في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ إيداع وثيقة الانضمام لدى الأمين العام لمجلس أوروبا.

المادة ٣٨ – التطبيق الإقليمي

١ .يجوز لأي دولة، وقت التوقيع على الاتفاقية أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، تحديد الإقليم أو الأقاليم التي تطبق عليها هذه الاتفاقية.

٢ .يجوز لأي دولة، في أي تاريخ لاحق، وبموجب إعلان موجه إلى الأمين العام لمجلس أوروبا، توسيع نطاق تطبيق هذه الاتفاقية على أي إقليم يتم تحديده في الإعلان. وتدخل الاتفاقية حيز التنفيذ بالنسبة لهذا الإقليم في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ استلام الإعلان من قبل الأمين العام لمجلس أوروبا.

٣ .يجوز سحب أي إعلان تم تقديمه بموجب الفقرتين السابقتين، بالنسبة لأي إقليم محدد في مثل هذا الإعلان، بموجب إشعار موجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب الإعلان حيز النفاذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام لمجلس أوروبا لهذا الإشعار.

المادة ٣٩ – الآثار المترتبة على الاتفاقية

١ .يتلخص الغرض من هذه الاتفاقية في استكمال المعاهدات أو الترتيبات ثنائية أو متعددة الأطراف فيما بين الأطراف، بما في ذلك أحكام:

-الاتفاقية الأوروبية بشأن تسليم المجرمين، التي فتحت للتوقيع بباريس في ١٣ ديسمبر/كانون الأول ١٩٥٧ (سلسلة المعاهدات الأوروبية رقم ٢٤)؛

-الاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية،التي فتحت للتوقيع بستراسبورغ في ٢٠ أبريل/نيسان ١٩٥٩ (سلسلة المعاهدات الأوروبية رقم ٣٠)؛

-البروتوكول الإضافي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية،التي فتحت للتوقيع بستراسبورغ في ١٧ مارس/آذار ١٩٧٨(سلسلة المعاهدات الأوروبية رقم ٩٩.

٢ .في حال إبرام طرفين أو أكثر لاتفاقية أو معاهدة بشأن المسائل التي تتناولها هذه الاتفاقية، أو إقامة علاقات بشأن مثل هذه المسائل بشكل آخر، أو عزمهم القيام بذلك في المستقبل، تكون تلك الدول مخولة لتطبيق تلك الاتفاقية أو

المعاهدة أو تنظيم علاقاتها بناء عليها. ومع ذلك، يجب على الدول الأطراف، في حال إقامة علاقات فيما يتعلق بالمسائل التي تتناولها هذه الاتفاقية بخلاف ما تنظمه هذه الاتفاقية، أن تنظم تلك العلاقات بطريقة تتفق مع أهداف الاتفاقية ومبادئها.

٣.لا يؤثر أي شيء ورد بهذه الاتفاقية على حقوق أي دولة طرف، قيودها، التزاماتها ومسئولياتها.

المادة ٤٠ – الإعلانات

يجوز لأي دولة، بموجب إعلان خطي يوجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، أن تعلن أنها تستفيد من إمكانية طلب عناصر إضافية كما هو منصوص عليه بموجب المواد ٢، ٣ و٦ – الفقرة ١(ب)، والمادة ٧، والمادة ٩ – الفقرة ٣، والمادة ٢٧ – الفقرة ٩ (هـ.

المادة ٤١ – البند الاتحادي

١ .يجوز للدولة الاتحادية الاحتفاظ بالحق في الاضطلاع بالالتزامات بموجب الباب الثاني من هذه الاتفاقية بما يتفق ومبادئها الأساسية التي تنظم

العلاقة بين حكومتها المركزية والدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة شريطة أن تظل قادرة على التعاون بموجب الباب الثالث.

٢ .لا يجوز للدولة الاتحادية، عند التحفظ بموجب الفقرة ١، تطبيق بنود هذا التحفظ لاستبعاد أو تقليص التزاماتها بشكل جوهري للتنصيص على التدابير المذكورة في الباب الثاني. وبشكل عام، يجب عليها توفير قدرة فعالة وواسعة في تنفيذ القانون فيما يتعلق بتلك التدابير.

٣ .بالنسبة لأحكام هذه الاتفاقية، التي يصبح تطبيقها بموجب الولاية القضائية للدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة غير الملزمة بالنظام الدستوري للاتحاد من أجل اتخاذ تدابير تشريعية، تقوم الحكومة الفيدرالية بإخبار السلطات المختصة في تلك الدول بالأحكام المذكورة إلى جانب رأيها المفضل، لتشجيعها على اتخاذ الإجراءات الملائمة لتفعيلها.

المادة ٤٢ – التحفظات

يجوز لأي دولة، بموجب إشعار خطي موجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، أن تعلن أنها تستفيد من التحفظ أو التحفظات المنصوص عليها في المادة ٤ – الفقرة ٢، والمادة

٦ –الفقرة ٣، والمادة ٩ – الفقرة ٤، والمادة ١٠ – الفقرة ٣، والمادة ١١ – الفقرة ٣، والمادة ١٤ – الفقرة ٣، والمادة

٢٢ –الفقرة ٢، والمادة ٢٩ – الفقرة ٤، والمادة ٤١ – الفقرة ١. ولا يجوز تقديم أية تحفظات أخرى.

المادة ٤٣ - الوضع التحفظات وسحبها

١ .يجوز لأي دولة طرف تقدمت بتحفظ طبقاً للمادة ٤٢ أن تسحب ذلك التحفظ كلياً أو جزئياً وذلك عن طريق إشعار خطي موجه إلى الأمين العام

لمجلس أوروبا. ويدخل سحب التحفظ حيز التنفيذ في تاريخ استلام الإشعار من قبل الأمين العام لمجلس أوروبا. وفي حال أشار الإشعار إلى تاريخ محدد لدخول سحب التحفظ حيز النفاذ، وكان ذلك التاريخ لاحقاً لتاريخ استلام الإشعار من قبل الأمين العام، يبدأ العمل بسحب التحفظ في ذلك التاريخ اللاحق.

٢ .يجوز لأي دولة طرف تقدمت بتحفظ كما هو مشار إليه في المادة ٤٢ سحب هذا التحفظ، كلياً أو جزئياً، بمجرد ما تسمح الظروف بذلك.

٣ .يجوز للأمين العام لمجلس أوروبا أن يستفسر، بشكل دوري، الدول الأطراف التي استخدمت تحفظا أو أكثر من تحفظ طبقاً للمادة ٤٢ عن احتمالات سحب ذلك التحفظ أو تلك التحفظات.

المادة ٤٤ – التعديلات

١ .يجوز لأي دولة طرف اقتراح تعديلات على هذه الاتفاقية، ويقوم الأمين العام لمجلس أوروبا بإرسالها إلى الدول الأعضاء بمجلس أوروبا، والدول غير الأعضاء التي شاركت في صياغة الاتفاقية، وكذلك إلى أي دولة انضمت إليها، أو تم توجيه الدعوة إليها للانضمام إلى هذه الاتفاقية وفقاً لأحكام المادة ٣٧.

٢ .يرسل أي تعديل مقترح من قبل دولة طرف إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، التي تعرض رأيها في هذا التعديل المقترح على لجنة الوزراء.

٣ .تنظر لجنة الوزراء في التعديل المقترح والرأي الذي تحيله عليها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) ، ويجوز لها، بعد التشاور مع الدول الأطراف غير الأعضاء في هذه الاتفاقية، تبني التعديل.

٤ .يرسل نص أي تعديل تتبناه لجنة الوزراء طبقاً للفقرة ٣ من هذه المادة إلى الدول الأطراف للموافقة عليه.

٥ .يدخل أي تعديل يتم إقراره طبقاً للفقرة ٣ من هذه المادة حيز التنفيذ في اليوم الثلاثين بعد إخبار جميع الدول الأطراف الأمين العام لمجلس أوروبا بقبولها بذلك التعديل.

المادة ٤٥ – تسوية النزاعات

١ .يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم بما يتعلق بتفسير وتطبيق هذه الاتفاقية. ٢. في حال حدوث نزاع بين دول أطراف بشأن تفسير أو تطبيق هذه الاتفاقية، يتيعن عليها السعي إلى تسوية للنزاع عبر التفاوض أو أي وسيلة سلمية أخرى من اختيارهم، بما في ذلك إحالة النزاع على اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) أو إلى هيئة تحكيم والتي تكون قرارتها ملزمة بالنسبة للأطراف، أو إلى محكمة العدل الدولية حسبما تتفق عليه الأطراف المعنيين.

المادة ٤٦ – مشاورات الأطراف

١ .تقوم الدول الأطراف، عند الاقتضاء، بالتشاور فيما بينها بشكل دوري بغية تيسير:

أ.الاستخدام والتنفيذ الفعال لهذه الاتفاقية، بما في ذلك تحديد أي مشاكل ذات الصلة، علاوة على آثار أي إعلان أو تحفظ يتم تقديمهما بموجب هذه الاتفاقية؛

ب. تبادل المعلومات بشأن التطورات القانونية، السياسية أو التكنولوجية ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في شكل إلكتروني؛

ج.دراسة الإضافات أو التعديلات الممكنة للاتفاقية.

٢ .يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم، بشكل دوري، بنتائج المشاورات المشار إليها في الفقرة ١.

٣ .تقوم اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) ، عند الاقتضاء، بتيسير المشاورات المشار إليها في الفقرة ١ واتخاذ التدابير اللازمة

لمساعدة الدول الأطراف في جهودها لاستكمال أو تعديل الاتفاقية. وتقوم اللجنة الأوروبية المعنية

بمشاكل الإجرام (CDPC) ، على الأكثر بعد ثلاث سنوات من دخول هذه الاتفاقية حيز التنفيذ، بالتعاون مع الدول الأطراف لإجراء مراجعة لكافة أحكام الاتفاقية، وعند الضرورة، تقدم توصيات بالتعديلات الملائمة.

٤ .بخلاف ما يتكفل به مجلس أوروبا، تلتزم الدول الأطراف بالنفقات الناجمة عن تنفيذ أحكام الفقرة ١ بالطريقة التي تحددها.

٥ .تساعد الأمانة العامة لمجلس أوروبا الدول الأطراف في تنفيذ مهامها طبقاً لهذه المادة.

المادة ٤٧ – الانسحاب

١ .يجوز لأي دولة طرف، في أي وقت، الانسحاب من هذه الاتفاقية عن طريق إشعار موجه إلى الأمين العام لمجلس أوروبا.

٢ .ويدخل هذا الانسحاب حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام للإشعار.

المادة ٤٨ – الإبلاغ

يقوم الأمين العام لمجلس أوروبا بإبلاغ الدول الأعضاء في مجلس أوروبا والدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية، علاوة على أي دولة انضمت إليها أو دعيت للانضمام إلى هذه الاتفاقية بـما يلي:

أ. أي توقيع؛

ب.إيداع أي صك للتصديق، القبول، الموافقة أو الانضمام؛

ج.أي تاريخ لدخول هذه الاتفاقية حيز التنفيذ طبقاً للمادتين ٣٦ و٣٧؛

د.أي إعلان يتم تقديمه بموجب المادة ٤٠ أو أي تحفظ يتم تقديمه طبقاً للمادة ٤٢؛ ه. أي إجراء، إخطار أو تواصل آخر يتعلق بهذه الاتفاقية.

وإثباتا لذلك، قام الموقعون أدناه، المفوضون بذلك حسب الأصول، بالتوقيع على هذه الاتفاقية.

حرر في بودابست – في الثالث والعشرين من شهر نوفمبر/تشرين الثاني ٢٠٠١، باللغتين الإنجليزية والفرنسية وكلا النصين متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا. ويرسل الأمين العام لمجلس أوروبا نسخا مصدقا عليها إلى كل دولة عضو في مجلس أوروبا، وإلى الدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية وإلى أي دولة دعيت للانضمام إليها.

قائمة المصادر والمراجع



أولا - قائمة المصادر:

النصوص القانونية:

1- القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، بتاريخ 2004/11/10.

2- القانون رقم 04/09 المؤرخ في 2009/08/5 المتضمن القواعد المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، بتاريخ 2009/08/16.

ثانيا - قائمة المراجع:

ا- المراجع باللغة العربية:

أ- الكتب:

1- برهان عزيزي، إثبات الجريمة في أحكام مجلة الاجراءات الجزائية، منشورات مجمع الأطرش للكتاب المختص: تونس، 2013.

2- طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على اجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات: الاسكندرية، 2016.

3- طه زاكي صافي، القواعد الجزائية العامة فقها واجتهادا،المؤسسة الحديثة للكتاب، طرابلس: لبنان، 1997.

4- عبد الصبور عبد القوي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع: القاهرة، الطبعة الأولى، 2008.

5- عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام)، دار موفم للنشر، الجزائر، 2009.

6- علاء عبد الباسط خلاف، الحماية الجنائية للحاسب الالكتروني والانترنت في ضوء (قانون العقوبات، قانون الاجراءات الجنائية، قانون حماية الملكية الفكرية، معهد الكويت للدراسات القضائية والقانونية، الطبعة الثانية، 2008، 2009.

7- غنية باطلي، الجريمة الالكترونية – دراسة مقارنة-، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.

8- فندوشي ربيعة، الاعلان الالكتروني، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011.

9- قشقوش هدى حامد، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

10- محمد حماد مرهج الهيتي، الجريمة المعلوماتية -دراسة مقارنة في التشريع الاماراتي والسعودي والبحريني والقطري والعماني-، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2014.

11- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الطبعة الأولى، دار الجامعة الجديدة، الاسكندرية.

12- محمد سيد سلطان، قضايا قانونية في أمن المعلومات والبيئة الالكترونية، دار ناشري للنشر الالكتروني، 2012.

13- نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر.

14- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2008.

ب- المذكرات والرسائل الجامعية:

❖ أطروحات الدكتوراه:

1- تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته"، رسالة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

2- محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2009/2008.

3- عصماني ليلى، التعاون الدولي لقمع الجرائم الدولية، رسالة الدكتوراه في القانون الدولي، جامعة وهران، 2013/2012

4- لحواطي عتيقة،استرجاع المعلومات العلمية والتقنية في ظل البيئة الرقمية ودوره في دعم الاتصال العلمي بين الباحثين، رسالة دكتوراه LMD في علم المكتبات، معهد علم المكتبات والتوثيق، جامعة قسنطينة،2014/2013.

❖ مذكرات الماجستير :

1- آمال قارة،الجريمة المعلوماتية، مذكرة ماجستير في الحقوق، كلية الحقوق، جامعة بن عكنون، الجزائر، 2001، 2002.

2- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011،2012.

3- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013.

4- عبد الله بن صالح بن رشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الاثبات بين الشريعة والقانون وتطبيقاتها في المملكة السعودية، مذكرة ماجستير في العدالة الجنائية، أكاديمية نايف للعلوم الأمنية، كلية الدراسات العليا.

5- عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية.

6- معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية، تخصص قانون جنائي وعلوم جنائية، جامعة باتنة، 2011، 2012.

7- منصور بن سعيد القحطاني، مهددات الأمن الالكتروني وسبل مواجهتها، رسالة ماجستير في العلوم الادارية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2008.

ج- المقالات العلمية المحكمة:

1- أسامة بن غانم العبيدي، (التفتيش عن الدليل في الجرائم المعلوماتية)، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، نوفمبر، ديسمبر 2013، المجلد 29، العدد 58.

2- خالد حامد مصطفى، (المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي)، رؤى استراتيجية،مركز الامارات للدراسات والبحوث الاستراتيجية، المجلد الأول، العدد 2، مارس 2013.

3- رضا هميسي، (تفتيش المنظومة المعلوماتية في القانون الجزائري)، مجلة العلوم القانونية والسياسية، عدد 5، جوان 2012.

4- سميرة معاشي، (ماهية الجريمة المعلوماتية)، مجلة المنتدى القانوني،قسم الكفاءة المهنية للمحاماة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد السابع، 2010.

5- سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، (الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهتها)، مجلة التقني، جامعة التعليم التقني، (العراق)، المجلد 24، العدد 9، 2011.

6- شوقي يعيش تمام، شبري عزيزة، (تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية)، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة بسكرة، عدد 15، سبتمبر 2017.

7- شوقي يعيش تمام، محمد خليفة، (نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري)، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، بيروت، لبنان، العدد 25، ماي 2018.

8- ضياء نعمان، (الحماية التقنية للتجارة الالكترونية)، مجلة قانون وأعمال، المطبعة والوراقة الوطنية، مراكش، المغرب، العدد 1، مارس 2011.

9- صفاء حسن نصيف، (التحديات الإجرائية المتصلة بالجرائم المعلوماتية)، مجلة العلوم القانونية والسياسية، جامعة بغداد، المجلد الخامس، العدد الثاني، 2016.

10- عادل يوسف عبد النبي الشكري، (الجريمة المعلوماتية وأزمة الشرعية الجزائية)، مجلة الكوفة، مركز دراسات الكوفة (العراق)، العدد السابع، 2008.

11- عبد الحليم بوقرين، (حتمية انشاء ضبطية خاصة بالجرائم الالكترونية)، مجلة العلوم القانونية والسياسية، جامعة تكريت، العراق، المجلد الخامس، العدد الأول، 2016.

12- فاضل عباس الملا، (الخطورة الأمنية للجرائم الإلكترونية وسبل مكافحتها)، مجلة كلية الجامعة الإسلامية، العدد 7، النجف العراق، 2009

13- ليتيم فتيحة، ليتيم نادية، (الأمن المعلوماتي للحكومة الالكترونية وإرهاب القرصنة)، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 12.

14- محمد بن فردية، (الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي، دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، السنة الخامسة، المجلد 09، العدد 01، 2014.

15- محمد علي سالم، حسون عبيد هجيج، (الجريمة المعلوماتية)، مجلة جامعة بابل للعلوم الانسانية جامعة بابل (العراق)، المجلد 14، العدد 3، 2008.

16- محمود وهيب، (ظاهرة العولمة وانعكاساتها الأمنية)، مجلة الأمن العام، المجلة العربية لعلوم الشرطة، العدد 164، القاهرة، مطابع الشرطة، يناير 1999.

17- مشتاق طالب وهيب، (مفهوم الجريمة المعلوماتية ودور الحاسب بارتكابها)، مجلة العلوم القانونية والسياسية، جامعة ديالي، (العراق)، المجلد الثاني، العدد 1، 2014.

18- ميسون خلف حمد الحمداني، (مشروعية الأدلة الإلكترونية في الإثبات الجنائي)، مجلة كلية الحقوق، جامعة النهرين، العراق، العدد 2، المجلد 18، 2016.

19- نوفل علي عبد الله الصفو، (جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، دراسة مقارنة)، المجلة المصرية للدراسات القانونية والاقتصادية، العدد الثالث، يناير2015 .

20- يزيد بوحليط، (تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري)، مجلة تواصل في الاقتصاد والإدارة والقانون، جامعة عنابة، عدد 48، ديسمبر 2016.

د- الملتقيات والبحوث والمؤتمرات العلمية:

1- أحمد عبد الرحمان البعادي، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، أيام 23 و24 و25 سبتمبر 2012، الخرطوم، السودان.

2- ألتريش سايبر، جرائم الكومبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، ترجمة سامي الشوي، دار النهضة العربية، القاهرة، مصر، 1993.

3- حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية، الملتقى الدولي الأول حول التنظيم القانوني للأنترنت والجريمة

الالكترونية، المنظم من طرف كلية الحقوق والعلوم السياسية، يومي 27 و28 أفريل، 2009 جامعة الجلفة.

4- ذياب موسى البداينة، الجرائم الالكترونية (المفهوم والأسباب)، ورقة علمية مقدمة الى الملتقى العلمي الموسوم ب: الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية 2014، عمان الأردن.

5- سيناء عبدالله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي، برنامج إدارة الحكم في الدول العربية POGAR -UNDP ، يومي 19 و20 يونيو 2007، المملكة المغربية.

6- فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبيرانية، دراسة شاملة عن مشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، فبراير 2013، فيينا.

هـ- المنشورات على شبكة الانترنت:

1- محمد ياسر أبو الفتوح، خصائص وتصنيفات الجريمة المعلوماتية، مقال منشور على الموقع الالكتروني: (تاريخ الزيارة: 11 /2017/11)

Almohakmoonalarab.ahlamontada.com/109-topic

2- يوسف قجاج، الجريمة الإلكترونية وإشكالية القواعد الإجرائية، منشور بالموقع: http://www.alkanounia.com، تاريخ الزيارة 02 جانفي 2017.

3- علي حسن الطوالبة، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، مركز الاعلام الأمني، ص 3، الموقع الالكتروني:

https://www.policemc.gov.bh/.../a79e37dc-9beb-4511-baec-21afff، تاريخ الزيارة 2017/12/15.

II - المراجع باللغة الأجنبية:

1 – European Crime Prevention Network, "Cybercrime: A theoretical overview of the growing digital threat", EUCPN Secretariat, February 2016, Brussels, available at: eucpn.org/sites/default/files/.../theoretical_paper_cybercrime_.pdf,

2 – Marc D. Goodman, "Why the Police don't care about computer crime", Harvard Journal of Law & Technology , Volume 10, Number 3 Summer 1997.

3 – W.Ph. Stol, J. Jansen, "Cybercrime and the Police", Published, sold and distributed by Eleven International Publishing, Printed in the Netherlands, 2013, available at: https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Cybercrime_and_the_Police.pdf

الفهرس

ملخص عام للمؤلف

أدى التوسع والتنوع في استخدام الوسائط الالكترونية في عصر البيئة الرقمية إلى تنامي التهديدات والانتهاكات الناتجة عن استغلال تلك الوسائط في مجالات الحياة المختلفة على نحو ما يضر بالمصالح الخاصة للأفراد كانتهاك سرية الحياة الخاصة أو سرية المراسلات، أو المصالح العامة للدولة كتزوير البيانات والمعطيات الالكترونية أو التجسس والقرصنة، وغيرها من صور تحت طائلة ما يعرف بالجريمة المعلوماتية التي مهما تعددت تسمياتها واختلف من تشريع لآخر إلا أن أثرها واحد.

وهو الأمر الذي دفع بالتشريعات الداخلية والدولية على البحث في كل مرة عن الحلول المجدية للتقليل من خطر الإجرام المعلوماتي إن لم نقل القضاء عليه نهائيا، وإن كنا لا ننكر في هذا الصدد أن الكثير من تلك المحاولات تعترضها عدة صعوبات موضوعية وإجرائية تعكس في النهاية خصوصية مكافحة الجريمة المعلوماتية.

وقد حاولنا من خلال هذا المؤلف الالمام بموضوع الجريمة المعلوماتية في سياقه التأصيلي من خلال ضبط مدلولها وخصائصها، وفي نفس الوقت تسليط الضوء على مختلف الصعوبات والاشكالات التي تعترض سبيل مكافحتها وفق ما هو مستقر عليه في أغلب التشريعات المقارنة، مع محاولتنا لطرح بعض الحلول التي نراها مجدية وممكنة لتجاوز عقبة مكافحة الجريمة المعلوماتية.

جامعة محمد خيضر - بسكرة
كلية الحقوق والعلوم السياسية
مخبر أثر الاجتهاد القضائي على حركة التشريع



صدر عن سلسلة مطبوعات المخبر:

1) الأعمـــال الإدارية ومنازعـــاتها.
الأستاذ الدكتور الزين عـــزري، 2010.

2) دليل إنجاز بحث تخرج في الحقوق.
الأستاذة الدكتورة حسينة شرون، 2017.

3) دراسات في الفكر الاستراتيجـــي.
الدكتـــورة نســـيمة طشوش، 2017.

4) أصـــول البحـــث العـــلمي.
مجموعة من المـــؤلفين، 2018.

5) الحقوق المدنية والسياسية (الواقع والرهانات)
مجموعة من المـــؤلفين، 2018.

جانفي 2019

الدكتور يعيش تمام شوقي
الجريمة المعلوماتية
جانفي 2019